NGUYỄN HỮU HOAN

SỐ HỌC PHỔ THÔNG

NHÀ XUẤT BẢN ĐẠI HỌC VÀ TRUNG HỌC CHUYÊN NGHIỆP
HÀ NỘI — 1986

ıg mỗi vấn đề ngoài nội dung cơ bản nói trên, mỗi khi được, chúng tôi còn giới thiệu những thành tựu lớn đã ; những bài toán hay đang còn chờ đợi lời giải.

ıối mỗi bài có nhiều bài tập đã được lựa chọn để bạn h luyện và củng cố chắc kiến thức đã đọc, một số bài tính chất bổ sung cho lý thuyết ngay trong bài đó hoặc thiết cho các bài sau. Tất cả các bài tập đều có đáp dẫn hoặc lời giải chi tiết.

. dung cuốn sách được trình bày hoàn toàn bằng toán p nhưng theo một sự lựa chọn và sắp xếp phù hợp với g khái niệm trong đại số hiện đại.

y vậy để hiểu được, bạn đọc chỉ cần có kiến thức toán íp hai bậc phổ thông, một số kiến thức về đa thức. Ngoài một số ký hiệu, chắc rằng bạn đọc có thể chóng làm quen hi đọc một vài trang đầu của cuốn sách.

hân đây tác giả xin bày tỏ lòng biết ơn đối với giáo sư Đức Thịnh và giáo sư Ngô Thúc Lanh đã giúp đỡ và góp :hi tiết nội dung cuốn sách. Tác giả cũng xin chân thành n ơn sự quan tâm giúp đỡ của các đồng chí trong tổ Đại số ıộc khoa Toán trường Đại học Sư phạm Hà Nội I, khi tác ıa viết cuốn sách này.

Chúng tôi không nghĩ rằng cuốn sách này đã được hoàn thiện ề mọi mặt, bởi vậy chúng tôi rất mong bạn đọc vui lòng chỉ ho những thiếu sót. Thư từ góp ý xin gửi về Nhà xuất bản Đại học và Trung học chuyên nghiệp 45 – Hàng Chuối, Hà Nội

NGUYỄN HỮU HOAN

MỞ ĐẦU

Trong cuốn sách này chúng tôi sẽ sử dụng một số kiến thức mà bạn đọc có thể đã quen biết ít nhiều. Chúng tôi nhắc lại ở đây để thống nhất với bạn đọc về các vấn đề đó.

1. Khái niệm tập hợp.

Chúng ta thường vẫn nói: Tập hợp các học sinh trong một lớp học; tập hợp các lớp trong một trường học, tập hợp các số tự nhiên: 0, 1, 2, 3,..., tập hợp các số nguyên: ..., – 3, – 2, – 1, 0, 1, 2, 3,...

Để chỉ rằng a là một vật của tập hợp A ta viết $a \in A$ và đọc « a là một phần tử của A » hoặc « a thuộc A ». Trong trường hợp a không là phần tử của A ta viết $a \notin A$.

Nếu mọi phần tử của tập hợp A đều là phần tử của tập hợp B thì ta viết $A \subset B$ hoặc $B \supset A$, đọc là « A là tập con của B » hoặc « A là một bộ phận của B » hoặc « B chứa A ». Bằng ký hiệu lôgic chúng ta diễn tả điều kiện $A \subset B$ là

$$\forall a : a \in A \Rightarrow a \in B.$$

Dấu « $\forall$ » có nghĩa là « tất cả » hay là « bất kỳ » hay là « mọi »; dấu « $\Rightarrow$ » có nghĩa là « kéo theo » hay là « suy ra ».

Hai tập hợp A và B được gọi là bằng nhau nếu như chúng chứa các phần tử y như nhau, nghĩa là mọi phần

tử thuộc A đều thuộc B và ngược lại. Khi ấy ta viết: A = B. Bằng ký hiệu lôgic ta có

$$A = B \Leftrightarrow A \subset B \text{ và } B \supset A.$$

Dấu « $\Leftrightarrow$ » chỉ sự tương đương lôgic giữa hai vế, tức là mỗi vế đều kéo theo vế kia và đọc là « khi và chỉ khi » hay là « nếu và chỉ nếu » hay là « cần và đủ ». Để chỉ một tập hợp không có phần tử nào ta viết ϕ, đọc là « rỗng ». Chẳng hạn tập hợp các nghiệm nguyên của phương trình $4x^2 - 1 = 0$ là rỗng. Viết $A = \phi$ có nghĩa « A là rỗng », còn viết $A \neq \phi$ nghĩa là A chứa ít nhất một phần tử nào đó. Như vậy

$$A \neq \phi \Leftrightarrow \exists a : a \in A.$$

Dấu « $\exists$ » đọc là « tồn tại » hay là « tất có » hay là « có ít nhất một ».

Nếu tập hợp A chỉ gồm một phần tử a thì ta viết $A = \{a\}$; nếu tập hợp A có hai phần tử a và b thì ta viết $A = \{a, b\}$ và nói chung $A = \{a, b, c, \ldots\}$ có nghĩa tập hợp A có các phần tử là a, b, c,...

Để diễn tả một tập con A của một tập hợp B được xác định bởi một tính chất τ nào đó ta viết:

$$A = \{x \in B \mid x \text{ có tính chất } \tau\},$$

và đọc là « A là tập hợp tất cả các phần tử x thuộc B, có tính chất τ ». Chẳng hạn:

$$A = \{x \in \mathbf{Z} \mid 2x^2 - 5x + 2 = 0\} \ (*)$$

diễn tả A là tập hợp các nghiệm nguyên của phương trình $2x^2 - 5x + 2 = 0$. Dễ thấy rằng $A = \{2\}$.

Cho hai tập hợp A và B tùy ý. Ký hiệu $A \cup B$ (đọc là « A hợp B ») là tập hợp gồm tất cả các phần tử hoặc thuộc A hoặc thuộc B; ký hiệu $A \cap B$ (đọc là « A giao B ») là tập hợp gồm tất cả các phần tử vừa thuộc A vừa thuộc B. Chẳng hạn

(*) Ký hiệu **Z** là tập hợp các số nguyên.

$$A = \{a, b, c, x, y\}$$
$$B = \{a, x, y, z\}$$

ta có

$$A \cup B = \{a, b, c, x, y, z\}$$
$$A \cap B = \{a, x, y\}.$$

2. Tổ hợp và nhị thức Niutơn.

Cho tập hợp A gồm n phần tử ($n \geq 2$). Mỗi một tập con gồm k phần tử của tập hợp A được gọi là một tổ hợp chập k của n phần tử đã cho. Chẳng hạn với $A = \{a_1, a_2, a_3, a_4\}$ ta có bốn tổ hợp chập 3 của 4 phần tử của A là $\{a_1, a_2, a_3\}$, $\{a_1, a_2, a_4\}$, $\{a_1, a_3, a_4\}$ và $\{a_2, a_3, a_4\}$. Để chỉ số tổ hợp chập k của n phần tử ta viết C_n^k. Ta có công thức

$$C_n^k = \frac{n(n-1)\dots(n-k+1)}{k!}.$$

Ở đây $k! = 1.2\dots k$ (đọc là « k giai thừa ») và để cho thuận tiện, người ta qui ước $0! = 1$.

Công thức sau đây được gọi là nhị thức Niu tơn:

$$(x+y)^n = C_n^0 x^n + C_n^1 x^{n-1} y + \dots + C_n^{n-1} x y^{n-1} + C_n^n y^n.$$

Vế phải của đẳng thức trên viết tắt là

$$\sum_{k=0}^{n} C_n^k x^{n-k} y^k$$

(đọc là « xích ma k từ 0 tới n của $C_n^k x^{n-k} y^k$ », nghĩa là tổng các hạng tử $C_n^k x^{n-k} y^k$, $k = 0, 1, \dots, n$.

3. Tập hợp số tự nhiên.

Trong tập hợp số tự nhiên $\mathbf{N} = \{0, 1, 2, \dots\}$ phép cộng và phép nhân luôn luôn thực hiện được, tuy nhiên phép trừ và phép chia cho số khác 0 không phải bao

giờ cũng thực hiện được. Với mỗi số tự nhiên a cho trước, bao giờ cũng có duy nhất một số tự nhiên bé nhất lớn hơn nó, đó là số $a+1$; gọi là số kề sau của a.

Chúng ta nêu lên một số kết quả quen thuộc sẽ được sử dụng trong cuốn sách này

Mệnh đề 1 *(Tiên đề qui nạp). Giả sử* $M \subset \mathbf{N}$ *thỏa mãn hai điều kiện*

1) $0 \in M$

2) $a \in M \Rightarrow a + 1 \in M$.

Khi ấy ta có $M = \mathbf{N}$.

Từ mệnh đề 1 suy ra hệ quả sau đây gọi là phép chứng minh qui nạp toán học.

Hệ quả. *Nếu mệnh đề toán học* $\mathcal{C}(n)$ *nào đó phụ thuộc vào số tự nhiên* n, *thỏa mãn các điều kiện:*

1) $\mathcal{C}(n)$ *đúng với* $n = 0$;

2) $\mathcal{C}(n)$ *đúng với số tự nhiên* $n = a$ *kéo theo* $\mathcal{C}(n)$ *đúng với* $n = a+1$

thì mệnh đề $\mathcal{C}(n)$ *đúng với tất cả các số tự nhiên n; nói khác đi* $\mathcal{C}(n)$ *là một định lý toán học.*

Đôi khi chúng ta còn dùng định lý về phép chứng minh qui nạp toán học dưới dạng khác.

Giả sử $\mathcal{C}(n)$ *là mệnh đề toán học nào đó phụ thuộc vào số tự nhiên* n *thỏa mãn* các điều kiện

1) $\mathcal{C}(k)$ *đúng*;

2) $\mathcal{C}(a)$ *đúng* $(a \geqslant k) \Rightarrow \mathcal{C}(a+1)$ *đúng.*

Khi ấy mệnh đề $\mathcal{C}(n)$ *đúng với tất cả các số tự nhiên* $n \geqslant k$.

Mệnh đề 2. *Giả sử* $M \subset \mathbf{N}$, $M \neq \phi$. *Khi ấy trong* M *có số nhỏ nhất, tức là* $\exists a \in M$ *sao cho* $a \leqslant x$, $\forall x \in M$.

Giả sử $M \subset \mathbf{N}$. Ta gọi M là bị chặn nếu như $\exists a \in \mathbf{N}$ sao cho $x \leqslant a$, $\forall x \in M$.

Mệnh đề 3. *Mọi bộ phận khác rỗng và bị chặn của tập hợp* **N** *các số tự nhiên đều có số lớn nhất.*

Mệnh đề 4. *(Nguyên tắc ngăn kéo của Diriclê). Nếu đem xếp hết tất cả* n *vật vào* n − 1 *ngăn kéo thì nhất thiết có một ngăn kéo nào đó chứa ít nhất hai vật.*

4. Tập hợp số nguyên.

Chúng ta thấy rằng tập hợp số nguyên $\mathbf{Z} = \{0, \pm 1, \pm 2, \ldots\}$ gồm tất cả các số tự nhiên và đối của tất cả các số tự nhiên. Trong tập hợp số nguyên các phép toán cộng, trừ và nhân luôn luôn thực hiện được, tuy nhiên phép chia cho số nguyên khác 0 không phải bao giờ cũng thực hiện được. Khác với tập hợp số tự nhiên, tập hợp số nguyên không có số nhỏ nhất.

Giả sử $M \subset \mathbf{Z}$. Ta gọi M là bị chặn trên nếu như $\exists a \in \mathbf{Z}$ sao cho $x \leqslant a$, $\forall x \in M$. Tương tự, ta gọi M là bị chặn dưới nếu như $\exists b \in \mathbf{Z}$ sao cho $b \leqslant x$, $\forall x \in M$. Tập hợp M được gọi là bị chặn nếu nó vừa bị chặn trên vừa bị chặn dưới. Ta có:

Mệnh đề 5. *Mọi bộ phận khác rỗng và bị chặn trên của tập hợp số nguyên* **Z** *đều có số lớn nhất. Mọi bộ phận khác rỗng và bị chặn dưới của tập hợp số nguyên* **Z** *đều có số nhỏ nhất.*

Giá trị tuyệt đối của số nguyên x là một số tự nhiên, ký hiệu là $|x|$ được xác định như sau:

$$|x| = \begin{cases} x & \text{nếu } x \in \mathbf{N}, \\ -x & \text{nếu } x \notin \mathbf{N}. \end{cases}$$

Ta có các hệ thức

$$-|x| \leqslant x \leqslant |x|;$$
$$||x| - |y|| \leqslant |x \pm y| \leqslant |x| + |y|;$$
$$|xy| = |x||y|; \ldots$$

LÝ THUYẾT CHIA HẾT TRONG VÀNH SỐ NGUYÊN

§ 1. TÍNH CHIA HẾT

I — ĐỊNH NGHĨA

Cho hai số nguyên a và b, $b \neq 0$. Ta nói *a chia hết cho b, hay b chia hết a* nếu như có số nguyên q sao cho $a = bq$, Khi ấy người ta còn nói a là bội của b hay b là *ước* của a và ký hiệu $a \vdots b$ hay $b \mid a$.

Chú ý: Nếu $b \mid a$ mà $a \neq 0$ thì từ $a = bq$ ta có $q \neq 0$ cho nên hiển nhiên $|a| = |b| |q| \geqslant |b|$ bởi vì $|q| \geqslant 1$.

II — TÍNH CHẤT

1. $b \mid a \Rightarrow \pm b \mid \pm a$;
2. $a \mid a$, $\forall a \in \mathbf{Z}$, $a \neq 0$;
3. $\pm 1 \mid a$, $\forall a \in \mathbf{Z}$. Ngoài ± 1 ra không còn số nguyên nào khác có tính chất này;
4. $0 \vdots a$, $\forall a \in \mathbf{Z}$, $a \neq 0$. Ngoài 0 ra không còn số nguyên nào khác có tính chất này;
5. $b \mid a$ và $a \mid b \Rightarrow a = \pm b$;
6. $a \mid b$ và $b \mid c \Rightarrow a \mid c$;
7. $c \mid a_i$, $i = 1, 2, \ldots, n \Rightarrow c \mid a_1x_1 + a_2x_2 + \ldots + a_nx_n$;
$x_i \in \mathbf{Z}$, $i = 1, 2, \ldots, n$.

Các tính chất trên đây được chứng minh dễ dàng, coi đó là những bài tập đơn giản. Ở đây chúng ta chứng minh tính chất 5 làm ví dụ. Từ $b \mid a$ và $a \mid b$ ta có $q, q' \in \mathbf{Z}$ sao cho $a = bq$ và $b = aq'$. Hai đẳng thức này cho ta $a = aqq'$ và do $a \neq 0$ ta có $qq' = 1$. Theo tính chất 3 ta phải có hoặc $q = q' = 1$ khi đó $a = b$; hoặc $q = q' = -1$ khi đó $a = -b$.

III — PHÉP CHIA CÓ DƯ

1. Định lý. *Cho hai số nguyên* a *và* b, $b \neq 0$. *Khi ấy có duy nhất cặp số nguyên* q, r *thỏa mãn các hệ thức*

$$a = bq + r \text{ và } 0 \leqslant r < |b|. \qquad (1)$$

Chứng minh. a) Có cặp số nguyên q, r thỏa mãn các hệ thức (1). Chúng ta xét tập hợp

$$M = \{bx \mid x \in \mathbb{Z}, bx \leqslant a\}.$$

Hiển nhiên $M \subset \mathbb{Z}$ và $M \neq \emptyset$ bởi vì $-|b|\,|a|$ là một bội của b không vượt quá a. Hơn nữa M bị chặn trên bởi a, nên theo mệnh đề 5, trong M có phần tử lớn nhất, chẳng hạn là bq, $q \in \mathbb{Z}$. Vì $|b| \geqslant 1$ nên $bq + |b| > bq$ từ đó $bq + |b| \notin M$. Hơn nữa $bq + |b|$ cũng là bội của b cho nên ta có

$$bq \leqslant a < bq + |b|$$

hay

$$0 \leqslant a - bq < |b|.$$

Bằng cách đặt $r = a - bq$ ta được $r \in \mathbb{Z}$, $a = bq + r$, $0 \leqslant r < |b|$.

b) Cặp số nguyên q, r thỏa mãn các hệ thức (1) là duy nhất. Thật vậy, giả sử có hai cặp số nguyên q, r và q_1, r_1 thỏa mãn các hệ thức (1), nghĩa là

$$a = bq + r,\ 0 \leqslant r < |b|;$$
$$a = bq_1 + r_1,\ 0 \leqslant r_1 < |b|.$$

Từ đây ta có $b(q - q_1) = r_1 - r$ và $|r_1 - r| < |b|$.

Khi ấy do $|b| > 0$ và $|b|\,|q - q_1| < |b|$ ta được $|q - q_1| < 1$. Song $|q - q_1|$ là một số tự nhiên nên từ $|q - q_1| < 1$ phải có $q - q_1 = 0$ hay $q_1 = q$ và kéo theo cả $r_1 = r$. Định lý được chứng minh hoàn toàn.

Trong các hệ thức (1) của định lý khi $r = 0$ thì $a = bq$ tức là a chia hết cho b, ta gọi q là *thương* trong phép

chia a cho b. Nếu $r \neq 0$ thì ta nói đó là phép chia có dư, r được gọi là số *dư*, q được gọi là số *thương hụt* trong phép chia a cho b.

§ 2. ƯỚC CHUNG LỚN NHẤT (UCLN)

I — ĐỊNH NGHĨA

— Một số nguyên được gọi là ước chung của các số nguyên $a_1, a_2, ..., a_n$ nếu nó là ước đồng thời của mỗi số đó.

— Một ước chung d của các số $a_1, a_2, ..., a_n$ sao cho mọi ước chung của $a_1, a_2, ..., a_n$ đều là ước của d được gọi là *ước chung lớn nhất* (viết tắt là UCLN) của các số đó.

— Nếu số 1 là ước chung lớn nhất của các số $a_1, a_2, ..., a_n$ thì ta nói các số $a_1, a_2, ..., a_n$ là *nguyên tố cùng nhau*. Còn nếu số 1 là ước chung lớn nhất của mọi cặp a_i, a_j với $i \neq j$; $i, j = 1, 2, ..., n$ thì ta nói các số $a_1, a_2, ..., a_n$ là *nguyên tố cùng nhau từng đôi một*, hay *nguyên tố sánh đôi*.

Chú ý. 1. Tập hợp các ước chung của nhiều số cho trước trùng với tập hợp các ước của UCLN của các số đó,

2. Ta biết số 1 là ước chung của mọi số nguyên, nên các số $a_1, a_2, ..., a_n$ bao giờ cũng có ước chung ít nhất là số 1. Số 0 là bội của mọi số nguyên khác 0 cho nên nếu tất cả các số $a_1, a_2, ..., a_n$ đều bằng 0 thì mỗi số nguyên khác 0 đều là ước chung của chúng, trong trường hợp này khái niệm UCLN không có nghĩa nữa. Do đó ta giả thiết rằng các số $a_1, a_2, ..., a_n$ đang xét không phải bằng 0 tất cả. Hơn nữa tập hợp tất cả các ước chung

của các số đang xét sẽ không thay đổi nếu ta thêm vào hay bớt đi các số bằng 0. Bởi vậy có thể giả thiết thêm $a_i \neq 0$ với mọi $i = 1, 2, ..., n$.

3. Nếu d là một UCLN của các số $a_1, a_2, ..., a_n$ thì $-d$ cũng là một UCLN của các số đó. Hơn nữa nếu d và d' là UCLN của các số $a_1, a_2, ..., a_n$ thì $d' = \pm d$. Do đó từ đây về sau nếu không có gì thay đổi, ta sẽ lấy số dương d trong các UCLN của $a_1, a_2, ..., a_n$ làm UCLN của chúng và ký hiệu $d = (a_1, a_2, ..., a_n)$.

4. Với chú ý 3) ta có thể định nghĩa: UCLN của các số nguyên $a_1, a_2, ..., a_n$ là số lớn nhất trong tập hợp các ước chung của chúng. Có thể chứng minh được rằng hai định nghĩa về UCLN đã nêu là tương đương, nếu không kể đến sự sai khác một thừa số ± 1.

II – ĐỊNH LÝ. *Có ước chung lớn nhất của các số nguyên khác không $a_1, a_2, ..., a_n$ cho trước.*

Chứng minh. Chúng ta xét tập hợp:

$$M = \{a_1x_1 + a_2x_2 + ... + a_nx_n / x_i \in \mathbb{Z}, i = 1, 2, ..., n\}.$$

Ta có $M \subset \mathbb{Z}$ và M chứa ít nhất một số nguyên dương, thật vậy, chẳng hạn lấy

$$x_k = \begin{cases} 1 \text{ với } a_k > 0, \\ -1 \text{ với } a_k < 0 \end{cases}$$

và $x_1 = x_2 = ... = x_{k-1} = x_{k+1} = ... = x_n = 0$ thì ta thấy rằng $a_1x_1 + a_2x_2 + ... + a_nx_n = |a_k| > 0$, $|a_k| \in M$. Bởi vậy trong M có số nguyên dương nhỏ nhất, chẳng hạn là d, nghĩa là

$d = a_1u_1 + a_2u_2 + ... + a_nu_n$, $u_i \in \mathbb{Z}$, $i = 1, 2, ..., n$ và $d \leqslant x$, $\forall x \in M$, $x > 0$.

Ta sẽ chứng minh $d = (a_1, a_2, ..., a_n)$. Trước hết ta thấy $d \mid x$, $\forall x \in M$. Thật vậy, $x \in M$ nên có các số nguyên $x_1, x_2, ..., x_n$ sao cho $x = a_1x_1 + a_2x_2 + ... + a_nx_n$. Giả sử

$x = dq + r$, $0 \leqslant r < d$, $r, q \in \mathbf{Z}$. Ta thấy rằng $r = 0$ vì nếu $0 < r < d$ thì

$$r = x - dq = a_1(x_1 - u_1q) + a_2(x_2 - u_2q) + \ldots + a_n(x_n - u_nq)$$

là một số nguyên dương nhỏ hơn d, thuộc M, trái với cách chọn số d. Từ $r = 0$ ta có $x = dq$, $q \in \mathbf{Z}$, nghĩa là $d \mid x$, $\forall x \in M$.

Bởi vì $a_k = a_1 0 + \ldots + a_{k-1}0 + a_k 1 + a_{k+1}0 + \ldots + a_n 0 \in M$ nên $d \mid a_k$, $k = 1, 2, \ldots, n$.

Mặt khác nếu $\delta \mid a_k$, $k = 1, 2, \ldots, n$ thì ta có $\delta \mid a_1u_1 + a_2u_2 + \ldots + a_nu_n$ tức là $\delta \mid d$. Vậy d là UCLN của $a_1, a_2, \ldots, a_n$ và định lý được chứng minh.

III – HỆ QUẢ

1. *Nếu $d = (a_1, a_2, \ldots, a_n)$ thì ắt có các số nguyên $u_1, u_2, \ldots, u_n$ sao cho $d = a_1u_1 + a_2u_2 + \ldots + a_nu_n$.*

Thật vậy, đây là hệ quả trực tiếp của cách chứng minh định lý trên.

2. *Điều kiện cần và đủ để $(a_1, a_2, \ldots, a_n) = 1$ là có các số nguyên $u_1, u_2, \ldots, u_n$ sao cho $1 = a_1u_1 + a_2u_2 + \ldots + a_nu_n$.*

Chứng minh. Nếu $(a_1, a_2, \ldots a_n) = 1$ thì theo hệ quả 1 ắt có $u_1, u_2, \ldots, u_n \in \mathbf{Z}$ sao cho $1 = a_1u_1 + a_2u_2 + \ldots + a_nu_n$.

Ngược lại nếu có $u_1, u_2, \ldots, u_n \in \mathbf{Z}$ thỏa mãn $1 = a_1u_1 + a_2u_2 + \ldots + a_nu_n$ thì mọi ước chung của $a_1, a_2, \ldots a_n$ đều là ước của 1, hơn nữa đương nhiên số 1 là ước chung của $a_1, a_2, \ldots, a_n$. Bởi vậy $(a_1, a_2, \ldots, a_n) = 1$.

3. a) *Với mọi số nguyên dương k ta có*

$$(ka_1, ka_2, \ldots, ka_n) = k.(a_1, a_2, \ldots, a_n).$$

b) *Nếu số dương δ là ước chung của các số $a_1, a_2, \ldots a_n$ thì ta có:*

$$\left(\frac{a_1}{\delta}, \frac{a_2}{\delta}, \ldots, \frac{a_n}{\delta}\right) = \frac{(a_1, a_2, \ldots, a_n)}{\delta}.$$

Chứng minh: a) Đặt $d = (a_1, a_2, \ldots, a_n)$ ta có d là số nguyên dương nhỏ nhất trong tập hợp

$$M = \{a_1x_1 + a_2x_2 + \ldots + a_nx_n \mid x_i \in \mathbf{Z}, i = 1, 2, \ldots, n\}.$$

Khi ấy rõ ràng kd là số nguyên dương nhỏ nhất trong tập hợp

$kM = \{(ka_1)x_1 + (ka_2)x_2 + ... + (ka_n)x_n / x_i \in Z, i = 1, 2, ..., n\}$ mà số nguyên dương nhỏ nhất trong tập hợp kM xác định như trên chính là $(ka_1, ka_2, ..., ka_n)$, cho nên ta có

$$(ka_1, ka_2, ..., ka_n) = k(a_1, a_2, ..., a_n).$$

b) Áp dụng kết quả a) của hệ quả trong trường hợp $\delta \mid a_i$ $i = 1, 2, ..., n$; $\delta > 0$ ta có

$$(a_1, a_2, ..., a_n) = \left(\delta . \frac{a_1}{\delta}, \delta . \frac{a_2}{\delta}, ..., \delta . \frac{a_n}{\delta}\right) =$$

$$= \delta\left(\frac{a_1}{\delta}, \frac{a_2}{\delta}, ..., \frac{a_n}{\delta}\right), \text{ cho nên}$$

$$\left(\frac{a_1}{\delta}, \frac{a_2}{\delta}, ..., \frac{a_n}{\delta}\right) = \frac{(a_1, a_2, ..., a_n)}{\delta}.$$

4. *Điều kiện cần và đủ để một ước chung dương d của các số $a_1, a_2, ..., a_n$ là UCLN của chúng là các số $\frac{a_1}{d}, \frac{a_2}{d}, ..., \frac{a_n}{d}$ nguyên tố cùng nhau.*

Chứng minh. Giả sử $d > 0$, $d \mid a_i$, $i = 1, 2, ..., n$. Khi ấy áp dụng hệ quả 3) ta có

$$d = (a_1, a_2, ..., a_n) \leftrightarrow d = d\left(\frac{a_1}{d}, \frac{a_2}{d}, ..., \frac{a_n}{d}\right) \leftrightarrow$$

$$1 = \left(\frac{a_1}{d}, \frac{a_2}{d}, ..., \frac{a_n}{d}\right).$$

IV – TÍNH CHẤT

1. *Nếu $(a, b) = 1$ và $b \mid ac$ thì $b \mid c$.*

Chứng minh: Từ $(a, b) = 1$ suy ra $\exists x, y \in Z$ sao cho $ax + by = 1$, từ đó $ac . x + bc . y = c$. Khi ấy do $b \mid ac$ và $b \mid bc$ ta có $b \mid acx + bcy$ tức là $b \mid c$.

2. Nếu $(a, b) = 1$ và c là một số nguyên tùy ý thì $(ac, b) = (c, b)$.

Chứng minh. Dựa vào chú ý 1) I, §2 ta chứng minh tập hợp các ước chung của ac và b trùng với tập hợp các ước chung của b và c. Giả sử $\delta \in \mathbb{Z}$, $\delta \mid ac$ và $\delta \mid b$. khi ấy $\delta \mid ac$ và $\delta \mid bc$, hay là $\delta \mid (ac, bc)$. Nhưng $(ac, bc) = (a, b)\, c = 1 . c = c$ nên $\delta \mid c$. Vậy ta có $\delta \mid b$ và $\delta \mid c$. Ngược lại, giả sử $\delta \in \mathbb{Z}$, $\delta \mid b$ và $\delta \mid c$ thì hiển nhiên ta có $\delta \mid b$ và $\delta \mid ac$.

3. Nếu $(a, b) = (a, c) = 1$ thì $(a, bc) = 1$.

Tổng quát : *nếu* $(a_i, b_j) = 1$, $i = 1, 2, \ldots, m$, $j = 1, 2, \ldots, n$ *thì* $(a_1 a_2 \ldots a_m, b_1 b_2, \ldots b_n) = 1$.

Chứng minh. Tính chất này là hệ quả của tính chất 2. bởi vì từ $(a, b) = 1$ ta có $(a, bc) = (a, c)$ nhưng $(a, c) = 1$. Trường hợp tổng quát lý luận tương tự, hoặc có thể chứng minh qui nạp.

V – CÁCH TÌM ƯỚC CHUNG LỚN NHẤT

1. Tìm ước chung lớn nhất của hai số : Cho hai số nguyên a và b, ta có thể giả thiết rằng $a > 0$, $b > 0$ và $a > b$.

a) Trường hợp $b \mid a$. Khi ấy ta có $(a, b) = b$. Thật vậy b là ước của a và b là ước của b nên b là ước chung của a và b hơn nữa mọi ước chung của a và b hiển nhiên là ước của b. Vậy $(a, b) = b$.

b) Trường hợp b không chia hết a.

Chú ý : *Với $a, b, c \in \mathbb{Z}$ sao cho $a = bq + c$, $q \in \mathbb{Z}$, ta có $(a, b) = (b, c)$.*

Thật vậy, mọi ước chung của a và b đều là ước của $c = a - bq$ nên cũng là ước chung của b và c. Ngược lại mọi ước chung của b và c đều là ước của $a = bq + c$ nên cũng là ước chung của a và b. Bởi vậy ta có $(a, b) = (b, c)$.

– *Thuật toán Ơclid.* Khi b không chia hết a thì ta có

$$a = bq + r_1, \qquad 0 < r_1 < b;$$
$$b = r_1q_1 + r_2, \qquad 0 < r_2 < r_1;$$
$$\dots\dots\dots\dots$$
$$r_{n-2} = r_{n-1}\,q_{n-1} + r_n, \qquad 0 < r_n < r_{n-1}$$
$$r_{n-1} = r_nq_n.$$

Dãy các phép chia liên tiếp này gọi là thuật toán Ơclid thực hiện trên hai số a và b. Số các phép chia này phải là hữu hạn và thuật toán Ơclid phải kết thúc với một số dư $r_{n+1} = 0$ vì dãy các số b, r_1, r_2,... là dãy các số tự nhiên giảm dần và do đó ta có không quá b phép chia.

Theo chú ý ở trên ta có $(a, b) = (b, r_1) = \dots = (r_{n-1}, r_n)$ và vì $r_{n-1} = r_nq_n$ nên theo kết quả a) thì $(r_{n-1}, r_n) = r_n$, do đó $(a, b) = r_n$. Nghĩa là : **UCLN của hai số a và b bằng số dư cuối cùng khác không trong thuật toán Ơclid thực hiện trên hai số đó.**

Ví dụ. Hãy tìm UCLN của 924 và 360.

Thực hiện thuật toán Ơclid trên hai số đó ta được

$$924 = 360 \,.\, 2 + 204,$$
$$360 = 204 \,.\, 1 + 156,$$
$$204 = 156 \,.\, 1 + 48,$$
$$156 = 48 \,.\, 3 + 12,$$
$$48 = 12 \,.\, 4.$$

Số dư cuối cùng khác 0 ở đây là 12. Vậy (924, 360) = 12. Trong thực hành người ta đặt phép tính như sau :

- 924 chia 360: số dư 204, thương 2
- 360 chia 204: số dư 156, thương 1
- 204 chia 156: số dư 48, thương 1
- 156 chia 48: số dư 12, thương 3
- 48 chia 12: số dư 0, thương 4

nên (924, 360) = 12.

2. Tìm ước chung lớn nhất của nhiều số. Cho các số nguyên dương $a_1, a_2, \ldots, a_n$ ta đặt $d = (a_1, a_2, \ldots, a_n)$ $(a_1, a_2) = d_2$, $(d_2, a_3) = d_3, \ldots, (d_{n-1}, a_n) = d_n$ thì ta có $d = d_n$.

Thật vậy ta dễ thấy rằng mọi ước chung của a_1, a_2 $a_3, \ldots a_n$ đều là ước chung của $d_2, a_3, \ldots a_n$ và ngược lại. Vì vậy ta có

$$(a_1, a_2, a_3, \ldots, a_n) = (d_2, a_3, \ldots, a_n).$$

Lặp lại lý luận này nhiều lần, ta sẽ được $(a_1, a_2, \ldots, a_n) = (d_2, a_3, \ldots, a_n) = (d_3, a_4, \ldots, a_n) = \ldots = (d_{n-1}, a_n) = d_n$ nghĩa là $d = d_n$.

Ví dụ. Hãy tìm UCLN của các số 924, 360 và 726 ta có

$$(924, 360, 726) = ((924, 360), 726) = (12, 726) = 6.$$

§ 3. BỘI CHUNG NHỎ NHẤT (BCNN)

I – ĐỊNH NGHĨA

– Ta gọi là *bội chung* của các số nguyên $a_1, a_2, \ldots, a_n$ một số nguyên là bội đồng thời của mỗi số đó.

– Một bội chung m của các số $a_1, a_2, \ldots, a_n$ sao cho mọi bội chung của $a_1, a_2, \ldots, a_n$ đều là bội của m gọi là *bội chung nhỏ nhất* (viết tắt là BCNN) của các số đó.

Chú ý. 1) Khi ta nói đến bội chung của các số $a_1, a_2, \ldots, a_n$ đương nhiên ta đã giả thiết các số đó khác 0.

2) Tập hợp các bội chung của nhiều số cho trước trùng với tập hợp các bội của BCNN của các số đó.

3) Nếu m là một BCNN của các số $a_1, a_2, \ldots, a_n$ thì $-m$ cũng là một BCNN của các số đó. Hơn nữa nếu m và m' là những BCNN của $a_1, a_2, \ldots, a_n$ thì $m' = \pm m$. Do đó từ đây về sau nếu không có gì thay đổi, ta sẽ lấy số dương m trong các BCNN của các số $a_1, a_2, \ldots, a_n$ làm và ký hiệu $m = [a_1, a_2, \ldots, a_n]$.

4) Với chú ý 3) ta có thể định nghĩa BCNN của các số nguyên $a_1, a_2, \dots, a_n$ là số nhỏ nhất trong tập hợp các bội chung dương của chúng. Có thể chứng minh được rằng hai định nghĩa về BCNN đã nêu là tương đương nếu không kể đến sự sai khác một thừa số ± 1.

II – ĐỊNH LÝ. *Có bội chung nhỏ nhất của các số nguyên khác không $a_1, a_2, \dots, a_n$ cho trước.*

Chứng minh: Chúng ta xét tập hợp

$$M = \{x \in \mathbf{Z} \mid x \,\vdots\, a_i, i = 1, 2, \dots, n\}.$$

Ta có $M \subset \mathbf{Z}$ và M chứa ít nhất một số nguyên dương, chẳng hạn số $|a_1 a_2 \dots a_n| \in M$. Bởi vậy trong M có số dương nhỏ nhất m, nghĩa là $m \,\vdots\, a_i$, $i = 1, 2, \dots, m > 0$ và $m \leqslant x$, $x \in M$, $x > 0$.

Ta sẽ chứng minh $m = [a_1, a_2, \dots, a_n]$.

Giả sử μ là một bội chung của $a_1, a_2, \dots, a_n$ và giả sử $\mu = mq + r$, $0 \leqslant r < m$, $q, r \in \mathbf{Z}$. Bởi vì $\mu \,\vdots\, a_i$, $m \,\vdots\, a_i$, $i = 1, 2, \dots, n$ nên $r = \mu - mq \,\vdots\, a_i$, $i = 1, 2, \dots, n$ tức là $r \in M$. Từ $r \in M$ với $0 \leqslant r < m$ và do tính chất của m là số dương nhỏ nhất thuộc M ta phải có $r = 0$ bởi vậy $\mu = mq$, nói khác đi mọi bội chung μ của các số $a_1, a_2, \dots, a_n$ đều là bội của m. Hơn nữa vì m là bội chung của các số $a_1, a_2, \dots, a_n$ nên ta có $m = [a_1, a_2, \dots, a_n]$.

III – TÍNH CHẤT

1. *Điều kiện cần và đủ để một bội chung dương m của các số $a_1, a_2, \dots, a_n$ là BCNN của chúng là các số $\frac{m}{a_1}, \frac{m}{a_2}, \dots, \frac{m}{a_n}$ nguyên tố cùng nhau.*

Chứng minh. a. *Điều kiện ắt có.* Cho biết m là BCNN của các số $a_1, a_2, \dots, a_n$ ta sẽ chứng minh $\frac{m}{a_1}, \frac{m}{a_2}, \dots, \frac{m}{a_n}$ là nguyên tố cùng nhau. Thật vậy, nếu không như thế, thì

các số $\frac{m}{a_1}, \frac{m}{a_2}, \ldots, \frac{m}{a_n}$ có một ước chung $d \neq \pm 1$ nào đó, khi đó $\frac{m}{d}$ là bội chung của $a_1, a_2, \ldots, a_n$ và $0 < \left|\frac{m}{d}\right| <$ m. Điều này trái với giả thiết m là BCNN của $a_1, a_2, \ldots, a_n$.

b) *Điều kiện đủ.* Cho biết $\frac{m}{a_1}, \frac{m}{a_2}, \ldots, \frac{m}{a_n}$ là các số nguyên tố cùng nhau, ta sẽ chứng minh m là BCNN của $a_1, a_2, \ldots, a_n$. Thật vậy, nếu không như thế, thì giả sử m' là BCNN của $a_1, a_2, \ldots, a_n$. Khi ấy ắt có số nguyên $d > 1$ để $m = dm'$. Từ đó ta có

$$\left(\frac{m}{a_1}, \frac{m}{a_2}, \ldots, \frac{m}{a_n}\right) = \left(\frac{dm'}{a_1}, \frac{dm'}{a_2}, \ldots, \frac{dm'}{a_n}\right) =$$

$$= d\left(\frac{m'}{a_1}, \frac{m'}{a_2}, \ldots, \frac{m'}{a_n}\right)$$

suy ra $d \,\Big|\, \left(\frac{m}{a_1}, \frac{m}{a_2}, \ldots, \frac{m}{a_n}\right)$, nghĩa là $\frac{m}{a_1}, \frac{m}{a_2}, \ldots, \frac{m}{a_n}$ có một ước chung $d > 1$, trái với giả thiết các số này là nguyên tố cùng nhau.

2. a) *Với k là một số nguyên dương, ta có*

$$[ka_1, ka_2, \ldots, ka_n] = k[a_1, a_2, \ldots, a_n].$$

b) Với số nguyên dương δ là một ước chung của các số $a_1, a_2, \ldots, a_n$ ta có

$$\left[\frac{a_1}{\delta}, \frac{a_2}{\delta}, \ldots, \frac{a_n}{\delta}\right] = \frac{[a_1, a_2, \ldots, a_n]}{\delta}.$$

Chứng minh. a) Đặt $m = [a_1, a_2, \ldots, a_n]$ theo cách chứng minh định lý ở II, ta có m là số nguyên dương nhỏ nhất của tập hợp

$$M = \{x \in Z \mid x \,\vdots\, a_i,\ i = 1, 2, \ldots, n\}.$$

Khi đó km sẽ là số nguyên dương nhỏ nhất của tập hợp

$$kM = \{kx \in Z \mid x \in Z,\ x \vdots a_i,\ i = 1, 2, \ldots, n\}.$$

Bởi vậy nếu ta chứng minh được tập hợp kM trùng với tập hợp

$$M_k = \{y \in Z \mid y \vdots ka_i,\ i = 1, 2, \ldots n\}$$

thì theo cách chứng minh định lý ở II, ta có

$$km = [ka_1, ka_2, \ldots, ka_n]$$

và ta được điều cần phải chứng minh.

Bây giờ ta chứng minh $kM = M_k$.

Thật vậy giả sử $\alpha \in kM$ ta có $\alpha = kx$, $x \in Z$ và $x \vdots a_i$, $i = 1, 2, \ldots, n$, khi đó $kx \vdots ka_i$, $i = 1, 2, \ldots, n$, nên $\alpha \in M_k$ nghĩa là $kM \subset M_k$.

Ngược lại giả sử $\alpha \in M_k$ ta có $\alpha \in Z$ và $\alpha \vdots ka_i$, $i = 1, 2, \ldots, n$ khi đó $\frac{\alpha}{k} \in Z$ và $\frac{\alpha}{k} \vdots a_i$, $i = 1, 2, \ldots, n$. Đặt $\frac{\alpha}{k} = x \in Z$ ta có $\alpha = kx$, $x \vdots a_i$, $i = 1, 2, \ldots, n$ nên $\alpha \in kM$, nghĩa là $M_k \subset kM$. Vậy tính chất a) được chứng minh.

b) Áp dụng kết quả a) với δ là ước chung dương của $a_1, a_2, \ldots, a_n$ ta có:

$$[a_1, a_2, \ldots, a_n] = \left[\delta . \frac{a_1}{\delta}, \delta . \frac{a_2}{\delta}, \ldots, \delta . \frac{a_n}{\delta}\right] = \delta \left[\frac{a_1}{\delta}, \frac{a_2}{\delta}, \ldots, \frac{a_n}{\delta}\right]$$

cho nên

$$\left[\frac{a_1}{\delta}, \frac{a_2}{\delta}, \ldots, \frac{a_n}{\delta}\right] = \frac{[a_1, a_2, \ldots, a_n]}{\delta}.$$

IV – CÁCH TÌM BỘI CHUNG NHỎ NHẤT

1. Tìm bội chung nhỏ nhất của hai số. Cho hai số nguyên a và b, giả thiết rằng $a > 0$, $b > 0$.

Ta có

$$[a, b] = \frac{ab}{(a, b)}.$$

Chứng minh. Ta gọi $m = \frac{ab}{(a, b)}$. Khi ấy bằng cách viết $m = a.\frac{b}{(a, b)} = b.\frac{a}{(a, b)}$ ta thấy m là một bội chung của a và b bởi vì các số $\frac{b}{(a, b)}$ và $\frac{a}{(a, b)}$ nguyên. Hơn nữa, giả sử μ là một bội chung tùy ý của a và b thì
$\frac{\mu}{m} = \mu.\frac{(a, b)}{ab} = \mu\frac{ax + by}{ab}$
với x và y là hai số nguyên sao cho $(a, b) = ax + by$ (2., III, §2). Từ đó ta có

$$\frac{\mu}{m} = \frac{\mu}{b}x + \frac{\mu}{a}y$$

là một số nguyên vì $\frac{\mu}{b}$ và $\frac{\mu}{a}$ là những số nguyên. Nói khác đi μ là một bội của m. Vậy $m = [a, b]$, và công thức được chứng minh.

Ví dụ. Hãy tìm BCNN của 84 và 90.

Ta có $(84, 90) = 6$ nên

$$[84, 90] = \frac{84 . 90}{6} = 1260.$$

2. Tìm bội chung nhỏ nhất của nhiều số. *Cho các số nguyên dương* $a_1, a_2, \ldots, a_n$. *Ta đặt* $m = [a_1, a_2, \ldots, a_m]$, $[a_1, a_2] = m_2$, $[m_2, a_3] = m_3, \ldots, [m_{n-1}, a_n] = m_n$ *thì ta có* $m = m_n$.

Thật vậy, vì tập hợp các bội chung của a_1 và a_2 trùng với tập hợp các bội của $[a_1, a_2] = m_2$ nên tập hợp các bội chung của $a_1, a_2, \ldots, a_n$ trùng với tập hợp các bội chung của $m_2, a_3, \ldots, a_n$. Vì vậy ta có:

$$[a_1, a_2, \ldots, a_n] = [m_2, a_3, \ldots, a_n].$$

Lặp lại lý luận này nhiều lần ta sẽ được:

$$[a_1, a_2, \ldots, a_n] = [m_2, a_3, \ldots, a_n] = [m_3, a_4, \ldots, a_n] = \ldots = \\ = [m_{n-1}, a_n] = m_n, \text{ nghĩa là } m = m_n.$$

Ví dụ: Tìm BCNN của các số 84, 90 và 165.

Ta có $[84, 90, 165] = [[84, 90], 165] =$

$$=[1260, 165] = \frac{1260 . 165}{(1260, 165)} = \frac{1260 . 165}{15} = 13860.$$

3. Hệ quả

a) *Nếu các số* $a_1, a_2, \ldots, a_n$ *nguyên tố cùng nhau từng đôi một thì BCNN của các số đó bằng tích* $a_1 a_2 \ldots a_n$ *của chúng.*

Chứng minh. Từ $(a_1, a_2) = 1$ ta có $m_2 = [a_1, a_2] = = \frac{a_1a_2}{(a_1, a_2)} = a_1a_2$. Theo giả thiết $(a_1, a_3) = (a_2, a_3) = 1$ nên $(m_2, a_3) = (a_1a_2, a_3) = 1$ do đó $m_3 = [m_2, a_3] = \frac{m_2a_3}{(m_2, a_3)} =$ $= m_2a_3 = a_1a_2a_3$.

Cứ tiếp tục như thế sẽ đi đến kết quả là

$$m = m_n = [a_1, a_2, \ldots, a_n] = a_1a_2\ldots a_n.$$

b) *Nếu số nguyên* x *là bội chung của nhiều số* $a_1, a_2, \ldots, a_n$ *nguyên tố cùng nhau từng đôi một thì* x *là bội của tích* $a_1a_2\ldots a_n$ *của chúng.*

Chứng minh: Thật vậy từ hệ quả a°) ta có

$$a_1a_2\ldots a_n = [a_1, a_2, \ldots, a_n]$$

mà $x \vdots a_i$, $i = 1, 2, \ldots, n$ thì $x \vdots [a_1, a_2, \ldots, a_n]$, nghĩa là $x \vdots a_1a_2\ldots a_n$.

BÀI TẬP

1.1. Trong định lý về phép chia có dư $a = bq + r$, $0 \leqslant r < b$ cho biết a, q hãy xác định b và r trong các trường hợp

a) $a = 335$, $q = 11$; b) $a = 1372$, $q = 128$.

1.2. Cho a, b, n là những số nguyên dương. Biết rằng với mỗi số nguyên dương k khác b đều có $k - b \mid k^n - a$. Chứng minh rằng $a = b^n$.

(Thi vô địch toán Cộng hòa Liên bang Nga năm 1964).

1.3. Chứng minh rằng

a) Trong $m+1$ số nguyên bất kỳ ắt có hai số có hiệu chia hết cho m.

b) Trong m số nguyên liên tiếp có một và chỉ một số chia hết cho m

1.4. Chứng minh rằng với số nguyên m ta có

a) $m^3 + 11m \vdots 6$; b) $m^5 - m \vdots 30$; c) $m^5 - 5m^3 + 4m \vdots 120$;

d) $3m^4 - 14m^3 + 21m^2 - 10m \vdots 24$.

1.5. Chứng minh rằng trong năm số nguyên tùy ý ắt có ba số mà tổng của chúng là bội của 3.

1.6. Chứng minh rằng với x và y là những số nguyên sao cho $x^2 + y^2$ chia hết cho 3 thì ta có x và y cùng chia hết cho 3.

1.7. Chứng minh rằng với $n \geqslant 1$ ta có

$$3(1^5 + 2^5 + \ldots + n^5) \vdots 1^3 + 2^3 + \ldots + n^3.$$

1.8. Chứng minh rằng với $n \geqslant 1$ và $k \geqslant 1$ là số lẻ, ta có $1^k + 2^k + \ldots + n^k \vdots 1 + 2 + \ldots + n$.

Nói riêng ta có

$$1^k + 2^k + \ldots + (2n)^k \vdots n(2n+1).$$

1.9. Chứng minh rằng

a) $11^{10} - 1 \vdots 100$; b) $2222^{5555} + 5555^{2222} \vdots 7$.

1.10. Chứng minh rằng với mọi $n \geqslant 1$ ta có

a) $16^n - 15n - 1 \vdots 225$; b) $3^{2^{4n+1}} + 2 \vdots 11$;

c) $5^{2n-1} \cdot 2^{n+1} + 3^{n+1} \cdot 2^{2n-1} \vdots 38$.

1.11. Chứng minh rằng nếu $a + b$ chia hết cho số tự nhiên lẻ n thì $a^n + b^n$ chia hết cho n^2.

1.12. Chứng minh rằng với $n \geqslant 1$ ta có :

a) $(n+1)^n - 1 \vdots n^2$; b) $2^{n(2^n - 1)} - 1 \vdots (2^n - 1)^2$.

1.13. Chứng minh rằng với $n \geqslant 1$ và k là số tự nhiên lẻ ta có

$$k^{2^n} - 1 \vdots 2^{n+2}.$$

1.14. Tìm tất cả các số tự nhiên n để $2^n - 1$ chia hết cho 7. Chứng minh rằng với mọi số tự nhiên n đều có $2^n + 1$ không chia hết cho 7.
(Thi vô địch toán Quốc tế — 1964)

1.15. Với những giá trị nào của số tự nhiên n thì
a) $3^n + 63$ chia hết cho 72? b) $n^{10} + 1$ chia hết cho 10?
c) $20^n + 16^n - 3^n - 1$ chia hết cho 323?

1.16. Cho hai dãy số
$a_n = 2^{2n+1} + 2^{n+1} + 1$,
$b_n = 2^{2n+1} - 2^{n+1} + 1$, $n = 0, 1, 2, \ldots$
Chứng minh rằng với mỗi số tự nhiên n có một và chỉ một trong hai số a_n, b_n chia hết cho 5.

1.17. Chứng minh rằng mỗi tổng sau đây không là số nguyên:

a) $A = \frac{1}{2} + \frac{1}{3} + \ldots + \frac{1}{n}$, $n > 1$;

b) $B = \frac{1}{3} + \frac{1}{5} + \ldots + \frac{1}{2n+1}$, $n > 0$.

1.18. a) Cho $(a, b) = 1$, $a > 1$, $b > 1$. Chứng minh rằng có duy nhất cặp số nguyên α, β thỏa mãn: $a\alpha - b\beta = 1$
$0 < \alpha < b$, $0 < \beta < a$.
b) Cho $(a, b) = 1$, $b > a > 1$ và k là một số tự nhiên sao cho $b \geqslant k > 1$. Chứng minh rằng có duy nhất cặp số nguyên α và β thỏa mãn: $a\alpha - b\beta = k$, $0 \leqslant \alpha < b$, $-1 \leqslant \beta < a$.

1.19. Chứng minh rằng:
a) $(a, a \pm b) = (a, b)$;
b) $(a \pm b, ab) = 1$ nếu $(a, b) = 1$;
c) $(2a + b, a(a + b)) = 1$ nếu $(a, b) = 1$;
d) $(5a + 3b, 13a + 8b) = (a, b)$.

1.20. Chứng minh rằng mỗi phân số sau đây là tối giản:

a) $\frac{21n + 4}{14n + 3}$; b) $\frac{n^3 + 2n}{n^4 + 3n^2 + 1}$; c) $\frac{m^2n + 2m}{mn + 1}$.

1.21. Tìm tất cả các cặp số tự nhiên a và b thỏa mãn
a) $a + b = 432$, $(a, b) = 36$; b) $ab = 8400$, $(a, b) = 20$;
c) $7a = 11b$, $(a, b) = 45$; d) $[a, b] = 2496$, $(a, b) = 24$.

1.22. Chứng minh rằng nếu $(a, n) = r$ và $(b, n) = s$ thì ta có $(ab, n) = (rs, n)$.

1.23. Cho $a \leqslant b \leqslant c$, $b = aq_1 + r_1$, $c = aq_2 + r_2$. Chứng minh rằng ta có

$$(a, b, c) = (a, r_1, r_2).$$

Áp dụng hãy tìm UCLN của các số 1218, 1794, 2730.

1.24. Cho a, b, c là các số lẻ. Chứng minh rằng ta có

$$(a, b, c) = \left(\frac{a+b}{2}, \frac{b+c}{2}, \frac{c+a}{2}\right).$$

Áp dụng hãy tìm UCLN của các số 1365, 2205, 4851.

1.25. Chứng minh rằng

a) với $a > 1$ ta có $(a^m - 1, a^n - 1) = a^{(m, n)} - 1$;

b) với $a > 1, m > 1$ ta có $\left(\frac{a^m - 1}{a - 1}, a - 1\right) = (a - 1, m)$;

c) với $a > 1$ ta có $(a! + 1, (a + 1)! + 1) = 1$.

1.26. Chứng minh rằng

a) nếu $0 < k < n$ và $(k, n) = 1$ thì C_n^k là bội của n;

b) nếu $(m, n) = 1$ thì ta có $\frac{(m+n-1)!}{m!\,n!}$ là một số nguyên.

Đặc biệt ta có $\frac{(2n)!}{n!(n+1)!}$ là một số nguyên.

1.27. Giả sử a, b là hai số nguyên lớn hơn 1 nguyên tố cùng nhau và m, n là hai số nguyên dương. Chứng minh rằng nếu $a^m + b^m$ chia hết cho $a^n + b^n$ thì m chia hết cho n.

1.28. Cho a, b là hai số nguyên dương nguyên tố cùng nhau và $ab = c^n$. Chứng minh rằng ắt có các số nguyên α, β sao cho $a = \alpha^n$, $b = \beta^n$, và $(\alpha, \beta) = 1$.

1.29. Chứng minh rằng dãy các số $a_n = 2^n - 3$ $(n = 2, 3, 4,...)$ chứa một tập hợp vô hạn các số đôi một nguyên tố cùng nhau.

(Thi vô địch toán quốc tế 1971).

1.30. Dãy $U_1, U_2, U_3,...$ được gọi là dãy các số *Phibônaxi* nếu $U_1 = U_2 = 1$, $U_m = U_{m-1} + U_{m-2}$ $(m = 3, 4,...)$

Chứng minh rằng:

a) $(U_n, U_{n+1}) = 1$;

b) $(U_m, U_n) = U_{(m, n)}$;

c) $U_n \mid U_m$ khi và chỉ khi $n \mid m$;

d) dãy số Phibônaxi chứa một tập hợp vô hạn các số đôi một nguyên tố cùng nhau.

1.31. Chứng minh rằng:

a) Dãy các *số tam giác* $t_n = \frac{1}{2} n(n+1)$, $n = 1, 2,\ldots$ chứa một tập hợp vô hạn các số đôi một nguyên tố cùng nhau;

b) Dãy các *số tứ diện* $T_n = \frac{1}{6} n(n+1)(n+2)$, $n = 1, 2,\ldots$ chứa một tập hợp vô hạn các số đôi một nguyên tố cùng nhau.

1.32. Tìm bội số chung nhỏ nhất của ba số tự nhiên liên tiếp.

1.33. Chứng minh rằng:

a) $[a, (b, c)] = ([a, b]; [a, c])$;

b) $(a, [b, c]) = [(a, b), (a, c)]$.

1.34. Chứng minh rằng

a) $[a, b, c] = \dfrac{abc\,(a, b, c)}{(a, b)(b, c)(c, a)}$;

b) $(a, b, c) = \dfrac{abc\,[a, b, c]}{[a, b][b, c][c, a]}$.

1.35. *Giả sử* $a_1, a_2,\ldots, a_n$ là những số nguyên dương. Đặt $a_1 a_2 \ldots a_n = A$ và $A_i = \dfrac{A}{a_i}$ $(i = 1, 2,\ldots, n)$. Chứng minh rằng:

a) $(a_1, a_2,\ldots, a_n)[A_1, A_2, \ldots, A_n] = A$,

b) $[a_1, a_2,\ldots, a_n](A_1, A_2,\ldots, A_n) = A$.

3. Định lý cơ bản. *Mỗi số tự nhiên lớn hơn 1 đều phân tích được thành một tích những thừa số nguyên tố và sự phân tích đó là duy nhất nếu không kể đến thứ tự các thừa số.*

Chứng minh. a) Giả sử a là số tự nhiên lớn hơn 1, ta hãy chứng minh rằng có thể phân tích a thành một tích của những thừa số nguyên tố. Thật vậy, vì $a > 1$ nên theo 3, I, số a có ít nhất một ước nguyên tố p_1 nào đó và ta đặt $a = p_1a_1$. Nếu $a_1 = 1$ thì ta có $a = p_1$ và đó là sự phân tích của a thành thừa số nguyên tố. Nếu $a_1 > 1$ thì cũng như trên, số a_1 có một ước nguyên tố p_1 nào đó và nếu ta đặt $a_1 = p_2a_2$ thì sẽ được $a = p_1p_2a_2$. Nếu $a_2 = 1$ thì ta có $a = p_1p_2$ và đó là sự phân tích của a thành thừa số nguyên tố. Nếu $a_2 > 1$ thì lại tiếp tục lí luận ở trên ta sẽ được số nguyên tố $p_3, \ldots$. Quá trình này phải kết thúc, nghĩa là ắt phải có n sao cho $a_{n-1} = p_n$ là số nguyên tố vì ta có $a, a_1, a_2, \ldots$ là một dãy số tự nhiên mà $a > a_1 > a_2 > \ldots$. Như vậy cuối cùng ta được $a = p_1p_2\ldots p_n$ là sự phân tích của a thành thừa số nguyên tố.

b) Bây giờ ta sẽ chứng minh sự phân tích trên của số a là duy nhất. Giả sử ta có

$$a = p_1p_2 \ldots p_n = q_1q_2 \ldots q_m$$

là hai dạng phân tích số a thành thừa số nguyên tố, thế thì ta có $p_1 \mid q_1q_2 \ldots q_m$ nên theo hệ quả ở trên $p_1 = q_i$ với i nào đó $(1 \leqslant i \leqslant m)$. Bằng sự đánh số lại ta giả sử $p_1 = q_1$ thì ta được:

$$p_2p_3 \ldots p_n = q_2q_3 \ldots q_m$$

Ta lấy p_2 và lắp lại lý luận trên ta được $p_2 = q_2$ và

$$p_3p_4 \ldots p_n = q_3q_4 \ldots q_m$$

Cứ tiếp tục như thế mãi cho tới khi đã ước lược hết các phần tử nguyên tố có chung ở hai vế của đẳng thức, ta phải có một vế nào đó bằng 1. Nhưng vì không thể xảy ra

$$1 = q_{n+1} q_{n+2} \dots q_m$$

hoặc

$$p_{m+1} p_{m+2} \dots p_n = 1$$

cho nên $m = n$ và như trên $p_i = q_i$, $i = 1, 2, \dots, n$. Từ đó tính duy nhất của dạng phân tích số a thành tích các thừa số nguyên tố đã được chứng minh.

4. Dạng phân tích tiêu chuẩn của số tự nhiên lớn hơn 1. Trong sự phân tích số $a > 1$ thành một tích những thừa số nguyên tố ở định lý cơ bản có thể xảy ra nhiều thừa số lặp lại. Gọi $p_1, p_2, \dots, p_k$ là các ước nguyên tố đôi một khác nhau của a và α_i $(1 \leqslant i \leqslant k)$ là số các nhân tử cùng là p_i trong sự phân tích của a thành một tích các thừa số nguyên tố thì ta có

$$a = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k} \qquad (1)$$

Khi ấy ta gọi (1) là *dạng phân tích tiêu chuẩn của số a*

Ví dụ: $1960 = 2^3 . 5 . 7^2$.

Định lý cơ bản nói lên vai trò quan trọng của số nguyên tố trong tập hợp số tự nhiên. Số nguyên tố là cơ sở nhân của tất cả các số tự nhiên lớn hơn 1. Chính vì vậy vấn đề số nguyên tố là một trong những vấn đề trung tâm của môn số học.

III – BẢNG SỐ NGUYÊN TỐ

1. Định lý (Ơclid). *Tập hợp các số nguyên tố là vô hạn.*

Chứng minh: Để chứng minh định lý này, chúng ta sẽ chứng tỏ rằng với bất kỳ n số nguyên tố nào cho trước $p_1, p_2, \dots, p_n$, $(n > 1)$ cũng ắt có số nguyên tố p

khác với n số nguyên tố đó. Thật vậy, ta hãy xét số $a = p_1p_2... p_n + 1$, đó là một số tự nhiên lớn hơn 1 nên ắt có số nguyên tố p là ước của a. Ta thấy p khác tất cả các số nguyên tố $p_1, p_2..., p_n$ bởi vì nếu p là một trong các số p_i $(1 \leqslant i \leqslant n)$ nào đó thì $p \mid p_1p_2... p_n$ và do $p \mid a = p_1p_2...p_n + 1$ nên ta được $p \mid 1$ là điều vô lý, và như vậy định lý được chứng minh.

Như vậy là ta không thể có một bảng tất cả các số nguyên tố. Nếu ta đánh số các số nguyên tố theo thứ tự tăng dần $p_1 = 2$, $p_2 = 3$, $p_3 = 5$,.... $p_n < p_{n+1}$.... thì cho đến nay người ta cũng chưa biết một biểu thức tổng quát nào cho số nguyên tố thứ n p_n theo chỉ số n của nó. Trong thực tế cần dùng, người ta lập nên các bảng số nguyên tố không vượt quá một số tự nhiên A nào đó.

2. Bổ đề. *Ước nhỏ nhất lớn hơn 1 của một hợp số a không vượt quá $\sqrt{a}$.*

Chứng minh: Gọi số tự nhiên p là ước nhỏ nhất lớn hơn 1 của a (đương nhiên theo 3, I., thì p là số nguyên tố) và giả sử $a = pa_1$ thế thì $p \leqslant a_1$. Nhân cả hai vế của bất đẳng thức $p \leqslant a_1$ với p ta có $p^2 \leqslant a_1p$ hay $p^2 \leqslant a$. Suy ra từ đó rằng $p \leqslant \sqrt{a}$ là điều cần phải chứng minh.

Từ bổ đề này ta suy ra một dấu hiệu về số nguyên tố, đó là hệ quả sau đây:

Hệ quả: *Nếu số tự nhiên $a > 1$ không có một ước nguyên tố nào trong khoảng từ 1 đến $\sqrt{a}$ thì a là số nguyên tố.*

Tuy nhiên để biết số tự nhiên $a > 1$ có là nguyên tố hay không ta cần phải biết tất cả các số nguyên tố trong khoảng từ 1 đến $\sqrt{a}$. Bây giờ chúng ta đi lập bảng các số nguyên tố không vượt quá một số tự nhiên $A \geqslant 1$ cho trước.

3. Lập bảng các số nguyên tố không vượt quá số tự nhiên A.

Ta viết tất cả các số tự nhiên từ 0 đến A, rồi tìm cách xóa đi trong bảng đó những số không phải là số nguyên tố, những số còn lại sẽ tạo nên bảng tất cả số nguyên tố không vượt quá A.

Trước hết ta xóa đi số 0 và số 1 vì hai số này không phải là số nguyên tố. Số đầu tiên chưa bị xóa là 2, đó là một số nguyên tố vì giữa 1 và 2 không còn một số tự nhiên nào cả nên 2 không có ước nào ngoài 1 và chính nó.

Ta giữ số 2 lại và xóa đi trong bảng tất cả những số khác là bội của 2, số đầu tiên bị xóa là $4 = 2^2$. Sau khi đã xóa hết các bội của 2 trong bảng thì số đầu tiên còn lại (số bé nhất lớn hơn 2) chưa bị xóa là 3, đó là một số nguyên tố vì nếu không thế thì 3 phải có một ước nguyên tố nhỏ hơn nó, ước ấy chỉ có thể là 2 và như vậy 3 là bội của 2 (mà khác 2) đã bị xóa.

Ta giữ số 3 lại và xóa đi trong bảng tất cả các số khác là bội của 3, số đầu tiên bị xóa là $9 = 3^2$ vì các bội khác của 3 mà nhỏ hơn 9 là 6 đã bị xóa với tư cách là bội của 2. Sau khi đã xóa hết các bội của 3 (khác 3) trong bảng, thì số đầu tiên còn lại (số bé nhất lớn hơn 3) chưa bị xóa là 5, đó là một số nguyên tố, vì nếu không thế thì 5 phải có một ước nguyên tố nào đó nhỏ hơn nó, ước ấy chỉ có thể là 2 hoặc 3 và như vậy 5 đã bị xóa với tư cách là bội của 2 hoặc 3.

Ta lặp lại quá trình trên đối với số nguyên tố 5 và các số nguyên tố sau số 5,... Việc làm như vậy khi nào sẽ kết thúc đối với một bảng các số tự nhiên $\leq A$? Ta có các kết quả sau đây:

— Sau khi đã xóa trong bảng tất cả bội của k số nguyên tố đầu tiên $p_1 = 2$, $p_2 = 3$, $p_3 = 5, ..., p_k$ (không

kể những số này) thì số đầu tiên còn lại chưa bị xóa sau p_k là số nguyên tố thứ $k + 1$ — p_{k+1}. Thật vậy nếu p_{k+1} không là nguyên tố thì nó phải có ít nhất một ước nguyên tố nhỏ hơn nó, ước ấy chỉ có thể là $p_1, p_2, \ldots, p_k$ (các số tự nhiên lớn hơn p_k và nhỏ hơn p_{k+1} đều là hợp số cả) và như vậy hóa ra p_{k+1} đã bị xóa.

— *Bội đầu tiên của số nguyên tố p_k (khác p_k) phải xóa là p_k^2* vì các bội khác của nó nhỏ thua p_k^2 là $2p_k$, $3p_k, \ldots, (p_k - 1)\, p_k$ đều đã bị xóa do các hợp số này có ước nguyên tố nhỏ nhất không phải là p_k mà nhỏ hơn p_k, còn p_k^2 chỉ có ước nguyên tố là p_k mà thôi.

— *Sau khi đã xóa tất cả các bội của $p_1 = 2$, $p_2 = 3$, $p_3 = 5, \ldots, p_n$ (không kể n số nguyên tố này) với điều kiện $p_n \leqslant A < p_{n+1}$ thì tất cả các số còn lại trong bảng chưa bị xóa đều là số nguyên tố cả.* Thật vậy, mọi hợp số $a \leqslant A$ đều có một ước nguyên tố $p < \sqrt{a} < \sqrt{A}$ cho nên p phải là một trong các số nguyên tố $p_1, p_2, p_3, \ldots p_n$, do đó a đã bị xóa với tư cách là bội của p.

Cách làm như trên để tìm tất cả các số nguyên tố không vượt quá một số tự nhiên cho trước gọi là « sàng Oratosten ».

Ví dụ: Lập bảng các số nguyên tố không vượt quá $A = 100$. Ta có $p_4 = 7$ là số nguyên tố lớn nhất không vượt quá $\sqrt{100}$, bởi vậy ta viết tất cả các số tự nhiên từ 2 đến 100 rồi xóa đi tất cả các bội của 2, 3, 5, 7 (không kể những số này) ta được bảng các số nguyên tố không vượt quá 100 (gồm 25 số):

	2	**3**	4	**5**	6	**7**	8	9	10
11	12	**13**	14	15	16	**17**	18	**19**	20
21	22	**23**	24	25	26	27	28	**29**	30
31	32	33	34	35	36	**37**	38	39	40
41	42	**43**	44	45	46	**47**	48	49	50
51	52	**53**	54	55	56	57	58	**59**	60

61	62	63	64	65	66	**67**	68	69	70
71	72	**73**	74	75	76	77	78	**79**	80
81	82	**83**	84	85	86	87	88	**89**	90
91	92	93	94	95	96	**97**	98	99	100

Từ bảng các số nguyên tố $\leqslant 100$ và dựa vào hệ quả ở trên ta có thể kiểm tra được rằng mỗi một số tự nhiên $a \leqslant 10000$ có phải là nguyên tố hay không. Muốn vậy ta lần lượt thử xem số $a > 1$ đó có một ước nguyên tố nào $\leqslant \sqrt{a}$ không, nếu a không có ước nguyên tố nào $\leqslant \sqrt{a}$ thì a là nguyên tố. Chẳng hạn xét số 257, ta có $\sqrt{257} < 17$, các số nguyên tố $\leqslant \sqrt{257}$ là 2, 3, 5, 7, 11, 13 đều không phải là ước của 257, nên 257 là số nguyên tố. Trong thực tế với những số không lớn lắm, muốn kiểm tra xem nó có phải là nguyên tố hay không người ta thường đối chiếu nó trong bảng các số nguyên tố.

Bảng số nguyên tố còn dùng để tìm dạng phân tích tiêu chuẩn của số tự nhiên $a > 1$. Muốn vậy dĩ nhiên ta cũng cần phải có một bảng gồm tất cả các số nguyên tố $\leqslant \sqrt{a}$. Nếu a không có một ước nguyên tố $\leqslant \sqrt{a}$ thì a là một số nguyên tố, nó chính là dạng phân tích tiêu chuẩn của a. Nếu a có ước nguyên tố $p \leqslant \sqrt{a}$ thì ta có $a = pa_1$ với $1 < a_1 < a$ ta lại tìm ước nguyên tố của a_1,... cứ thế mãi sau một số hữu hạn bước ta sẽ được dạng phân tích tiêu chuẩn của số a.

Trong thực hành, chẳng hạn để tìm dạng phân tích tiêu chuẩn của số 1960 ta đặt tính như sau :

1960	2
980	2
490	2
245	5
49	7
7	7
1	

ta được $1960 = 2^3 . 5 . 7^2$

Ngay từ thế kỷ XVII Kataldi (1603) đã lập bảng các số nguyên tố < 760. Shuten (1657) đã lập bảng các số nguyên tố $< 10\,000$.

Vào những năm cuối thế kỷ XIX, I.M Pervushin đã lập bảng các số nguyên tố < 10000000. Ông đã dành trên 40 năm (1854 – 1897) của cuộc đời cho công trình này. Đó là bảng số nguyên tố lớn nhất thời bấy giờ, phải viết trong 750 tờ giấy đầy chữ nhỏ.

Gần đây, năm 1959 K.L. Baker và F.Grunberger đã lập bảng tất cả 6 triệu số nguyên tố đầu tiên. Số nguyên tố thứ 6.000.000 là 104395301. Hiện nay bảng số nguyên tố đầy đủ nhất và lớn nhất là các bảng của Kulik (ở dạng bản thảo) – cho đến 100 330 201 và bảng của Baker và của Grunberger (bằng microphim) – cho đến 104395301.

Với bảng các số nguyên tố không vượt quá A như thế người ta có thể tìm được dạng phân tích tiêu chuẩn của bất cứ số tự nhiên không vượt quá $a = A^2$.

Vấn đề phân tích một số tự nhiên thành dạng tiêu chuẩn, cũng như vấn đề xét xem một số tự nhiên có phải là nguyên tố hay không, về mặt nguyên tắc đã được giải quyết hoàn toàn, nhưng trong thực tế, đối với các số lớn vấn đề này không phải là đơn giản vì như vậy là phải thực hiện khá nhiều phép tính. Bởi vậy « nói chung » thì người ta chưa biết được rằng một số tự nhiên a cho biết, là nguyên tố hay hợp số. Cho đến năm 1983, số nguyên tố lớn nhất mà người ta biết được là số $2^{86243} - 1$, nó gồm 25962 chữ số trong hệ ghi số thập phân.

IV – MỘT VÀI ỨNG DỤNG

1. Tiêu chuẩn chia hết

Định lý. *Cho a là một số tự nhiên với dạng phân tích tiêu chuẩn là:*

$$a = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}.$$

Khi ấy số tự nhiên d là ước của a khi và chỉ khi nó có dạng

$$d = p_1^{\beta_1} p_2^{\beta_2} \ldots p_k^{\beta_k}$$

với $0 \leqslant \beta_i \leqslant \alpha_i$, $i = 1, 2, \ldots, k$.

Chứng minh. Giả sử d | a, nghĩa là có số nguyên q sao cho a = dq. Đẳng thức này chứng tỏ rằng nếu d > 1 thì mọi ước nguyên tố của d là ước nguyên tố của a và số mũ của ước nguyên tố ấy trong dạng phân tích tiêu chuẩn của d không lớn hơn số mũ của nó trong dạng phân tích tiêu chuẩn của a. Bởi vậy

$$d = p_1^{\beta_1} p_2^{\beta_2} \ldots p_k^{\beta_k},\ 0 \leqslant \beta_i \leqslant \alpha_i,\ i = 1, 2, \ldots, k;$$

nếu d = 1 thì ta có thể viết $d = p_1^{\beta_1} p_2^{\beta_2} \ldots p_k^{\beta_k}$, $\beta_i = 0$, $i = 1, 2, \ldots k$.

Ngược lại giả sử a và d là hai số tự nhiên thỏa mãn điều kiện của định lý, khi ấy $\alpha_i - \beta_i \geqslant 0$, $i = 1, 2, \ldots, k$ nên $q = p_1^{\alpha_1 - \beta_1} p_2^{\alpha_2 - \beta_2} \ldots p_k^{\alpha_k - \beta_k}$ là một số tự nhiên và a = dq, nghĩa là d | a.

Chú ý. a) Định lý này cho ta *cách xác định tất cả các ước của một số tự nhiên a > 1*, muốn vậy trong biểu thức

$$d = p_1^{\beta_1} p_2^{\beta_2} \ldots p_k^{\beta_k}$$

ta chỉ việc cho β_i $(i = 1, 2, \ldots, k)$ độc lập với nhau lấy các giá trị $0, 1, \ldots, \alpha_i$. Ví dụ với $a = 140 = 2^2 . 5 . 7$ ta có $d = 2^{\beta_1} 5^{\beta_2} 7^{\beta_3}$ với $\beta_1 = 0, 1, 2$, $\beta_2 = 0, 1$; $\beta_3 = 0, 1$ cụ thể ta được các ước của 140 là 1, 2, 4, 5, 7, 10, 14, 20, 28, 35, 70, 140.

b) Từ định lý trên ta suy ra kết quả là *nếu số tự nhiên a > 1 có dạng phân tích tiêu chuẩn* $a = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_k^{\alpha_k}$ *thì số các ước của a là* $(\alpha_1 + 1)(\alpha_2 + 1) \ldots (\alpha_k + 1)$.

c) *Giả sử a và b là hai số tự nhiên khác 0, nguyên tố cùng nhau. Khi ấy số tự nhiên d là ước của tích ab khi*

và chỉ khi $d = xy$ trong đó x là ước của a, y là ước của b và x, y nguyên tố cùng nhau.

Thật vậy, nếu ít nhất trong hai số a và b có một số bằng 1 thì kết quả là hiển nhiên, bởi vì chẳng hạn $a = 1$ ta có $ab = b$ và $d \mid ab$ khi và chỉ khi $d = 1 . y$ trong đó $y \mid b$. Nếu a và b cùng lớn hơn 1 thì giả sử

$$a = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_r^{\alpha_r} \text{ và } b = q_1^{\gamma_1} q_2^{\gamma_2} \ldots q_s^{\gamma_s}$$

là phân tích tiêu chuẩn của a và b. Khi ấy từ giả thiết $(a, b) = 1$ ta có $p_1, p_2, \ldots, p_r, q_1, q_2, \ldots, q_s$ là những số nguyên tố khác nhau và

$$ab = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_r^{\alpha_r} \; q_1^{\gamma_1} q_2^{\gamma_2} \ldots q_s^{\gamma_s}$$

là dạng phân tích tiêu chuẩn của số ab. Theo định lý trên thì $d \mid ab$ khi và chỉ khi

$$d = p_1^{\beta_1} p_2^{\beta_2} \ldots p_r^{\beta_r} \; q_1^{\delta_1} q_2^{\delta_2} \ldots q_s^{\delta_s}$$

$0 \leqslant \beta_i \leqslant \alpha_i$ $(i = 1, 2, \ldots, p)$, $0 \leqslant \delta_j \leqslant \gamma_j$ $(j = 1, 2, \ldots, s)$, trong đó $x = p_1^{\beta_1} p_2^{\beta_2} \ldots p_r^{\beta_r}$ là ước của a, $y = q_1^{\delta_1} q_2^{\delta_2} \ldots q_s^{\delta_s}$ là ước của b và $(x, y) = 1$.

2. Ước chung lớn nhất. Ta sẽ sử dụng dạng phân tích tiêu chuẩn của các số tự nhiên để tìm ước chung lớn nhất và bội chung nhỏ nhất của nhiều số.

Cho $a_1, a_2, \ldots, a_n$ là những số tự nhiên lớn hơn 1, gọi $p_1, p_2, \ldots, p_k$ là các ước nguyên tố phân biệt của ít nhất một trong các số $a_1, a_2, \ldots, a_n$ ta có thể viết

$$a_i = p_1^{\alpha_{i1}} p_2^{\alpha_{i2}} \ldots p_k^{\alpha_{ik}}$$

$\alpha_{ij} \geqslant 0$; $i = 1, 2, \ldots, n$; $j = 1, 2, \ldots, k$ ($\alpha_{ij} > 0$ nếu như $p_j \mid a_i$ và $\alpha_{ij} = 0$ nếu như p_j không chia hết a_i). Khi ấy số

$$d = p_1^{\mu_1} p_2^{\mu_2} \ldots p_k^{\mu_k}, \text{ với } \mu_j = \min_{1 \leqslant j \leqslant k} \{\alpha_{1j}, \alpha_{2j}, \ldots, \alpha_{nj}\}$$

là số nhỏ nhất trong các số $\alpha_{1j}, \alpha_{2j}, \ldots, \alpha_{nj}$, sẽ là UCLN của $a_1, a_2, \ldots, a_n$.

Thật vậy, từ giả thiết về μ_j ta có với mọi $i = 1, 2, \ldots, n$ $\mu_j \leqslant \alpha_{ij}$ cho nên theo 1) số d là ước chung của $a_1, a_2, \ldots, a_n$. Mặt khác giả sử δ là một ước chung nào đó của $a_1, a_2, \ldots, a_n$ theo 1) thì δ phải có dạng $\delta = p_1^{\beta_1} p_2^{\beta_2} \ldots p_k^{\beta_k}$ với $0 \leqslant \beta_j \leqslant \alpha_{ij}$; $i = 1, 2, \ldots, n$, $j = 1, 2, \ldots, k$, nghĩa là $\beta_j \leqslant \mu_j$ cho nên δ là ước của d. Vậy d là UCLN của $a_1, a_2, \ldots, a_n$ từ đó ta có:

UCLN của nhiều số $a_1, a_2, \ldots, a_n$ là một số d là tích lũy thừa các thừa số nguyên tố chung của tất cả các số $a_1, a_2, \ldots, a_n$, mỗi thừa số mang số mũ nhỏ nhất của nó trong các dạng phân tích tiêu chuẩn của các số đã cho $a_1, a_2, \ldots, a_n$.

Ví dụ $1960 = 2^3.5.7^2$, $2352 = 2^4.3.7^2$, $4004 = 2^2.7.11.13$,

ta có: $d = (1960, 2352, 4004) = 2^2.7 = 28$.

3. Bội số chung nhỏ nhất. Cũng bằng ký hiệu đã có ở trên ta có

$$m = p_1^{\rho_1} p_2^{\rho_2} \ldots p_k^{\rho_k}, \text{ với } \rho_j = \max \{\alpha_{1j}, \alpha_{2j}, \ldots, \alpha_{nj}\}$$

là số lớn nhất trong các số $\alpha_{1j}, \alpha_{2j}, \ldots, \alpha_{nj}$ sẽ là BCNN của $a_1, a_2, \ldots, a_n$.

Thật vậy với giả thiết về ρ_j và theo 1) ta có m là một bội chung của $a_1, a_2, \ldots, a_n$ và mỗi bội chung v của $a_1, a_2, \ldots, a_n$ đều là bội của m cho nên m là BCNN của $a_1, a_2, \ldots, a_n$ và ta có:

BCNN của nhiều số $a_1, a_2, \ldots, a_n$ là một số m là tích lũy thừa các thừa số nguyên tố chung và riêng của các số $a_1, a_2, \ldots, a_n$, mỗi thừa số mang số mũ lớn nhất của nó trong dạng phân tích tiêu chuẩn của các số đã cho $a_1, a_2, \ldots, a_n$.

Ví dụ: $m = [1960, 2352, 4004] = 2^4.3.5.7^2.11.13 = 1681680$

và định lý đã được chứng minh. Tuy nhiên ta thấy rằng ước giá này còn quá thô sơ vì chẳng hạn $p_4 < 2^{2^3} = 256$, trong khi đó $p_4 = 7$.

Người ta cũng đã chứng minh được rằng $p_n \leqslant 2^{n+1}$ và hơn thế nữa $p_n \leqslant 2^{n-1} + 2$ song các kết quả này cũng còn rất thô sơ vì chẳng hạn $p_{10} = 29$ trong khi đó số nguyên tố lớn nhất không vượt quá $2^{10-1} + 2 = 514$ là $p_{97} = 509$.

Một kết quả định tính lớn nhất mà người ta đã tìm được ở cuối thế kỷ trước là

$$\lim_{n \to \infty} \frac{p_n}{n \ln n} = 1$$

($\ln n$ là logarit cơ số e của n).

c) Về vấn đề này Sièpinski cho ta định lý sau đây để xác định số nguyên tố p_n. Nếu

$$\alpha = \sum_{n=1}^{\infty} p_n \cdot 10^{-2^n} \quad \text{thì}$$

$$p_n = [10^{2^n} \cdot \alpha] - 10^{2^{n-1}}[10^{2^{n-1}} \cdot \alpha] \; (*)$$

Định lý này cho ta một công thức đơn giản để xác định số nguyên tố p_n song đòi hỏi phải xác định được α, mà muốn thế ta lại phải biết tất cả các số nguyên tố, bởi vậy nó chỉ có ý nghĩa lý thuyết mà thôi.

2. Một vấn đề đơn giản nữa đặt ra là: *Có hay không một biểu thức chỉ lấy giá trị là các số nguyên tố với mọi giá trị tự nhiên của ẩn*. Cho đến nay cũng chưa hy vọng chỉ ra được một biểu thức như vậy.

a) *Biểu thức đó là một đa thức*. Ta có « đa thức Ơle » $p(x) = x^2 + x + 41$. Với $x = 0, 1, 2, ..., 39$ đa thức Ơle cho ta các giá trị nguyên tố 41, 43, 47, ..., 1601, nhưng

---

(*) $[x]$ là số nguyên lớn nhất không vượt quá số thực x (xem § 1, bài thứ ba).

chưa biết rằng có hay không một số tự nhiên $m > 41$ sao cho với $x = 0, 1, 2, \ldots, m-2$, $f(x) = x^2 + x + m$ cho những giá trị đều là số nguyên tố. Ta cũng thấy rằng đa thức $x^2 - 79x + 1601$ lấy các giá trị nguyên tố với $x = 0, 1, 2, \ldots, 79$. Tuy nhiên không khó khăn lắm ta có thể chứng minh được rằng không có một đa thức nào với hệ số nguyên lấy giá trị nguyên tố với mọi giá trị tự nhiên của ẩn.

Người ta đặt vấn đề xét xem *có hay không một đa thức lấy vô số giá trị nguyên tố?* Đối với nhị thức bậc nhất thì ta có định lý: *mọi đa thức bậc nhất $ax+b$ với $(a, b) = 1$ đều lấy vô số giá trị nguyên tố.* Hơn thế nữa người ta cũng đã chứng minh được rằng với a xác định và $b < a$ thì các số nguyên tố dạng $ax + b$ « phân bố đều cho b ». Chẳng hạn với $a = 4$, ta có vô số số nguyên tố dạng $4x + 1$ và có vô số số nguyên tố dạng $4x + 3$ và số các số nguyên tố trong hai loại này là « tương đương ».

Đối với nhị thức bậc nhất thì vấn đề được giải quyết như vậy, còn đối với các đa thức bậc cao hơn 1 thì người ta chưa tìm được một đa thức nào lấy vô số giá trị nguyên tố. Có giả thuyết cho rằng các đa thức $x^2 + x + 41$, $x^2 - 79x + 1601$, $x^2 + 1$, $x^2 + 2$ lấy vô số giá trị nguyên tố.

b) *Số Phécma.* Phécma phát biểu rằng các số $F_n = 2^{2^n} + 1$ với $n = 0, 1, 2, \ldots$ đều là nguyên tố cả. Các số F_n được gọi là *số Phecma.*

Dễ dàng chứng minh được rằng nếu $k > 0$ thì điều kiện cần để số $2^k + 1$ là nguyên tố là k phải có dạng 2^n. Tuy nhiên điều ngược lại không đúng vì Ơle đã chứng minh được rằng $F_5 = 2^{2^5} + 1$ có ước nguyên tố là 641. Ơle cũng đã chứng minh được rằng ước nguyên tố của $F_n = 2^{2^n} + 1$ phải có dạng $t \cdot 2^{n+2} + 1$.

Đến năm 1952 người ta đã biết các số Phécma $F_n = 2^{2^n} + 1$ là hợp số với n = 5, 6, 7, 8, 9, 11, 12, 18, 23, 36, 38, 73. Nhờ máy tính điện tử đến năm 1964 người ta đã biết thêm với n = 10, 13, 14, 15, 16, 19, 21, 25, 26, 27, 30, 32, 39, 42, 52, 55, 58, 63, 77, 81, 117, 125, 144, 150, 207, 226, 228, 260, 267, 268, 284, 316, 452, 1945 có $F_n = 2^{2^n} + 1$ là hợp số. Hợp số Phécma F_{1945} có hơn 10^{582} chữ số trong hệ ghi số thập phân, ước nguyên tố nhỏ nhất của F_{1945} là số $5.2^{1947} + 1$ gồm 587 chữ số trong hệ ghi số thập phân.

Tuy nhiên cho đến nay cũng chưa biết tập hợp số nguyên tố Phécma cũng như tập hợp hợp số Phécma là vô hạn hay hữu hạn.

Việc nghiên cứu các số nguyên tố Phéc ma là bổ ích bởi vì các số Phéc ma có liên quan mật thiết đến bài toán chia một vòng tròn ra làm những phần đều nhau bằng thước kẻ và compa. Gauss đã chứng minh được rằng *có thể chia một vòng tròn cho trước ra làm n phần đều nhau bằng thước kẻ và com-pa khi và chỉ khi* $n = 2^a \times p_1 . p_2 ... p_k$ *trong đó* $a \geq 0$ *và* $p_1, p_2, ..., p_k$ *là những số nguyên tố Phéc ma phân biệt.*

c) *Số Méc.xen.* Các số dạng $M_n = 2^n - 1$ được gọi là *số Méc.xen.*

Có thể chứng minh dễ dàng nếu n là hợp số thì M_n cũng là hợp số, vì vậy nếu M_n là nguyên tố, thì n cũng phải là nguyên tố. Tuy nhiên điều ngược lại không đúng, bởi vì $M_{11} = 2^{11} - 1 = 2047 = 23.89$.

Nếu số Mécxen là nguyên tố thì người ta gọi số đó là *số nguyên tố Mécxen.* Cho đến năm 1971 người ta đã biết được các số Mécxen $M_p = 2^p - 1$ là số nguyên tố với p = 2, 3, 5, 7, 13, 17, 19, 31, 61, 89, 107, 127, 521, 607, 1279, 2203, 3217, 4253, 4423, 9689, 9941, 11213, 19937. Bắt đầu từ chỉ số p = 521, số nguyên tố Mécxen Mp được kiểm

tra bằng máy tính điện tử (năm 1952). Số nguyên tố $M_{19937} = 2^{19937} - 1$ gồm có 6002 chữ số trong hệ ghi số thập phân, nó là số nguyên tố lớn nhất mà năm 1971 người ta biết được. Năm 1979 D.Slovinski phát hiện số nguyên tố Mecxen thứ 27 M_{44497} và tháng 1 năm 1983 D.Slovinski lại phát hiện số nguyên tố Mécxen $M_{86243} = 2^{86243} - 1$. Số nguyên tố Mecxen M_{86243} gồm 25962 chữ số trong hệ ghi cơ số thập phân, người ta chưa biết nó có phải là số nguyên tố Mécxen thứ 28 hay không, nhưng có điều chắc chắn nó là số nguyên tố lớn nhất mà lúc ấy con người biết được.

Đến nay bài toán tập hợp các số nguyên tố Mécxen là vô hạn hay hữu hạn cũng chưa giải được.

Số nguyên tố Mécxen có ý nghĩa quan trọng là vì nó liên quan mật thiết với các số hoàn chỉnh mà trong bài thứ ba chúng ta sẽ có dịp đề cập đến.

d) Về vấn đề tìm biểu thức cho số nguyên tố, cách đây khoảng ba chục năm (1947) người ta đã chứng minh được các định lý sau đây :

– Có một số thực α *sao cho* $[\alpha^{3^n}]$ *lấy giá trị nguyên tố với mọi số tự nhiên* $n > 0$.

– Có một số thực $\alpha = \alpha_0$ *sao cho các số* $[2^{\alpha_0}], [2^{\alpha_1}], \ldots$ *xác định bởi công thức qui nạp* $\alpha_{n+1} = 2^{\alpha_n}$ *đều là số nguyên tố.*

Tuy nhiên các định lý này cũng chỉ có ý nghĩa lý thuyết mà thôi.

3. Sự phân bố số nguyên tố. Để nghiên cứu sự phân bố số nguyên tố trong dãy số tự nhiên, người ta xét hàm số $\pi(x)$. Theo định nghĩa, $\pi(x)$ biểu thị số các số nguyên tố không vượt quá số thực dương x. Ví dụ, $\pi(1.37) = 0$, $\pi(2) = 1$, $\pi(10) = 4$, $\pi(p_n) = n$.

Từ định nghĩa ta có ngay hệ thức $0 \leqslant \pi(x) < x$, và theo định lý Ơclid về tính vô hạn của tập hợp các số

Hãy xét xem khi chia số nguyên tố cho 60 thì có kết quả như trên không ?

b) Chứng minh rằng nếu tổng của n lũy thừa bậc 4 của các số nguyên tố lớn hơn 5 là một số nguyên tố thì n phải nguyên tố cùng nhau với 30.

2.5. Xác định số nguyên tố p sao cho $2p + 1$ là lập phương của một số tự nhiên.

2.6. Tìm tất cả các số nguyên tố p sao cho nó vừa là tổng của hai số nguyên tố nào đó, vừa là hiệu của hai số nguyên tố nào đó.

2.7. Tìm tất cả các số nguyên tố p sao cho tổng tất cả các ước tự nhiên của p^4 là một số chính phương.

2.8. Với mỗi số tự nhiên s, $2 \leqslant s \leqslant 10$, hãy tìm tất cả các số nguyên tố p sao cho $1 + p$ là lũy thừa bậc s của một số tự nhiên.

2.9. Chứng minh rằng có nhiều vô hạn cặp các số nguyên m và n khác nhau sao cho m và n có cùng các ước nguyên tố, và $m + 1$ và $n + 1$ có cùng các ước nguyên tố.

2.10. Chứng minh rằng với n là một số lẻ lớn hơn 1, các số n và $n + 2$ cùng là nguyên tố khi và chỉ khi $(n - 1)!$ không chia hết cho n và $n + 2$.

2.11. Chứng minh rằng có vô số cặp số nguyên tố liên tiếp mà không phải là cặp số nguyên tố sinh đôi.

2.12. a) Cho p và $8p^2 + 1$ là những số nguyên tố. Chứng minh rằng $8p^2 + 2p + 1$ cũng là số nguyên tố.

b) Cho $p > 5$ là một số nguyên tố, biết rằng $2p + 1$ cũng là số nguyên tố. Chứng minh $4p + 1$ là hợp số.

2.13. Chứng minh rằng với $m > 2$ giữa m và m! có ít nhất một số nguyên tố. Từ đó suy ra rằng có vô số số nguyên tố.

2.14. Tìm tất cả các số nguyên tố p sao cho $p + 6$, $p + 8$, $p + 12$ và $p + 14$ cũng là những số nguyên tố.

2.15. a) Chứng minh rằng tích của các số tự nhiên dạng $4m + 1$ lại là một số tự nhiên dạng ấy. Từ đó suy ra rằng có nhiều vô hạn các số nguyên tố dạng $4m + 3$.

b) Giải bài toán tương tự cho trường hợp các số nguyên tố dạng $6m + 5$

2.16. Tìm tất cả các số nguyên tố dạng $\frac{n(n+1)}{2} - 1$ với $n > 1$.

2.17. Tìm tất cả các số nguyên tố dạng $\frac{n(n+1)(n+2)}{6} + 1$ với $n \geqslant 1$.

2.18. Tìm tất cả các cấp số cộng nhiều hơn hai số hạng mà mỗi số hạng đều là nguyên tố với công sai d trong những trường hợp sau :

a) d là một số lẻ ; b) $d = 2$; c) $d = 10$; d) $d = 6$ mà cấp số cộng có nhiều hơn 4 số hạng.

2.19. Chứng minh rằng với các số nguyên tố lớn hơn 3 lập thành cấp số cộng nhiều hơn hai số hạng thì công sai phải là bội của 6.

2.20. a) Tìm tất cả các số nguyên $k \geqslant 0$, với chúng dãy $k+1, k+2, \ldots, k+10$ chứa nhiều số nguyên tố nhất.

b) Giải bài toán tương tự với dãy $k+1, k+2, \ldots, k+100$.

2.21. Chứng minh rằng không có một đa thức một ẩn nào với hệ số nguyên lấy giá trị nguyên tố với mọi giá trị tự nhiên của ẩn.

2.22. Giả sử p_n là số nguyên tố thứ n. Chứng minh rằng.

a) Không có đa thức f(x) với hệ số nguyên nào mà $f(1) = p_1$, $f(2) = p_2$ và $f(3) = p_3$.

b) Với mỗi số tự nhiên $m > 1$ ắt có một đa thức f(x) với hệ số hữu tỷ thỏa mãn $f(k) = p_k$ với $k = 1, 2, \ldots, m$.

c) Với mỗi số tự nhiên $m > 1$ ắt có một đa thức f(x) với hệ số nguyên sao cho $f(p_k) = p_k$ với $k = 1, 2, \ldots, m$.

2.23. a) cho $2^k + 1$ là một số nguyên tố. Chứng minh rằng hoặc $k = 0$ hoặc $k = 2^n$ với n là một số tự nhiên.

b) cho $2^k - 1$ là một số nguyên tố. Chứng minh rằng k là số nguyên tố.

2.24. Chứng minh rằng với $n > 2$, các số $2^n + 1$ và $2^n - 1$ không thể cùng là nguyên tố.

2.25. Chứng minh rằng với $m \neq n$ ta có $(F_m, F_n) = 1$, trong đó $F_k = 2^{2^k} + 1$, $k = 0, 1, 2, \ldots$. Từ đó suy ra rằng có vô số số nguyên tố.

2.26. Cho $F_k = 2^{2^k} + 1$, $k = 0, 1, 2, \ldots$ Chứng minh rằng

a) $F_{n+1} = 2 + F_0 F_1 \ldots F_n$;

b) $F_n \mid 2^{F_n} - 2$.

2.27. Chứng minh rằng có nhiều vô hạn các số lẻ $k > 0$ với chúng tất cả các số $2^{2^n} + k$ $(n \geqslant 1)$ là hợp số.

2.28. Chứng minh rằng trong dãy các số Méexen $M_n = 2^n - 1$ $(n \geqslant 1)$ có khoảng dài tùy ý gồm toàn hợp số.

2.29. Chứng minh rằng với n là một số tự nhiên chẵn lớn hơn 4, ta có các số Mecxen $M_n = 2^n - 1$ là tích của ít nhất ba thừa số tự nhiên khác 1.

2.30. Chứng minh rằng hai mệnh đề sau đây là tương đương với nhau:

a) Chỉ có hữu hạn số nguyên tố Méexen và hữu hạn số nguyên tố Phécma;

b) Chỉ có hữu hạn số tự nhiên m sao cho mỗi số m và m + 1 chỉ có một ước số nguyên tố.

BÀI THỨ BA

MỘT VÀI HÀM SỐ SỐ HỌC

§ 1. PHẦN NGUYÊN VÀ PHẦN PHÂN CỦA MỘT SỐ THỰC

I – ĐỊNH NGHĨA

1. Phần nguyên của số thực x, ký hiệu bởi [x] là số nguyên lớn nhất không vượt quá x. Như vậy [x] là số nguyên thỏa mãn.

$$[x] \leqslant x < [x] + 1.$$

Ví dụ : $[3] = 3$; $[\pi] = 3$; $[-2,71] = -3$; $\left[\frac{10}{3}\right] = 3$

2. Phần phân của số thực x, ký hiệu bởi $\{x\}$ là hiệu của x trừ đi $[x]$:

$$\{x\} = x - [x].$$

Ví dụ : $\{3\} = 0$; $\{\pi\} = 0,14159 \ldots$;

$\{-2,71\} = 0,29$; $\left\{\frac{10}{3}\right\} = \frac{1}{3}$.

Hệ quả. *Ta có* $0 \leqslant \{x\} < 1$.

II – TÍNH CHẤT

1. Cho α *là một số thực dương và d là một số tự nhiên khác không. Khi ấy các số tự nhiên khác 0 là bội của d mà không vượt quá* α *bằng* $\left[\frac{\alpha}{d}\right]$.

Chứng minh. Thật vậy, gọi m là số các số tự nhiên khác 0 là bội của d mà không vượt quá α, thì các số tự nhiên đó phải là d, 2d, ..., md và

$$md \leqslant \alpha < (m+1)\,d$$

hay là

$$m \leqslant \frac{\alpha}{d} < m + 1$$

Theo định nghĩa của hàm số phần nguyên hệ thức sau cùng này chứng tỏ rằng $m = \left[\frac{\alpha}{d}\right]$.

Ta có thể diễn đạt tính chất 1 bởi hệ thức

$$\sum_{\substack{0 < k \leqslant \alpha \\ k \,\vdots\, d}} 1 = \left[\frac{\alpha}{d}\right].$$

2. Cho α *là một số thực tùy ý và* **d** *là một số tự nhiên khác không. Khi ấy ta có đẳng thức*

$$\left[\frac{[\alpha]}{d}\right] = \left[\frac{\alpha}{d}\right].$$

Chứng minh. Đặt $m = \left[\frac{\alpha}{d}\right]$ ta phải chứng minh $\left[\frac{[\alpha]}{d}\right] = m$. Thật vậy ta có

$$m \leqslant \frac{\alpha}{d} < m + 1$$

nên
$$md \leqslant \alpha < (m + 1)d$$

Từ đó hiển nhiên ta có

$$md \leqslant [\alpha] < (m + 1)d$$

và sau khi chia tất cả cho $d > 0$ ta được

$$m \leqslant \frac{[\alpha]}{d} < m + 1.$$

Hệ thức sau cùng này chứng tỏ $\left[\frac{[\alpha]}{d}\right] = m$.

3. *Cho n là một số tự nhiên lớn hơn 1. Khi ấy số mũ α_p của số nguyên tố p cho trước trong dạng phân tích tiêu chuẩn của n! bằng*

$$\alpha_p = \left[\frac{n}{p}\right] + \left[\frac{n}{p^2}\right] + \left[\frac{n}{p^3}\right] + \cdots$$

Chứng minh. Trước hết ta chú ý rằng tổng trên đây để xác định α_p không phải gồm vô hạn số hạng. Thật vậy vì $p \geqslant 2$ nên ắt có số tự nhiên k khác 0 sao cho $p^k \leqslant n < p^{k+1}$, do đó $\left[\frac{n}{p^i}\right] = 0$ với mọi $i > k$ và tổng trên chỉ gồm có k số hạng

Bây giờ ta chứng minh định lý. Ta thấy rằng trong tích $n! = 1.\ 2 \ldots.\ n$ có và chỉ có $\left[\frac{n}{p}\right]$ thừa số là bội của p (theo tính chất 1), đó là các thừa số

$$p,\ 2p, \ldots, \left[\frac{n}{p}\right]p.$$

Lũy thừa của p trong n! chỉ do từ các số này mà ra. Ta hãy nhân các số này với nhau và tìm lũy thừa của p trong tích số đó. Ta được tích số đó là

$$p \cdot 2p \dots \left[\frac{n}{p}\right] p = p^{\left[\frac{n}{p}\right]} \cdot \left[\frac{n}{p}\right]!$$

Lúc này vấn đề lại là tìm số mũ của p trong phân tích tiêu chuẩn của $\left[\frac{n}{p}\right]!$ Bài toán đặt ra đúng như bài toán đang giải, nhưng $\left[\frac{n}{p}\right] < n$. Lặp lại lý luận ở trên với chú ý rằng:

$$\left[\frac{\left[\frac{n}{p}\right]}{p}\right] = \left[\frac{n}{p^2}\right] \text{ (theo tính chất 2)}$$

ta được tích các bội của p trong tích $\left[\frac{n}{p}\right]!$ là

$$p \cdot 2p \dots \left[\frac{n}{p^2}\right] \cdot p = p^{\left[\frac{n}{p^2}\right]} \left[\frac{n}{p^2}\right]!.$$

Lặp lại lý luận trên với $\left[\frac{n}{p^2}\right]!$ và tiếp tục như thế cho tới khi nào ta được $\left[\frac{n}{p^k}\right] < p$. Cuối cùng ta được

$$\alpha_p = \left[\frac{n}{p}\right] + \left[\frac{n}{p^2}\right] + \left[\frac{n}{p^3}\right] + \dots$$

Viết gọn lại là

$$\alpha_p = \sum_{i=1}^{k} \left[\frac{n}{p^i}\right].$$

trong đó k là số tự nhiên sao cho $p^k < n < p^{k+1}$

Ví dụ : Tìm số mũ α_p của số nguyên tố p trong phân tích tiêu chuẩn của 1000 ! với p = 2, p = 5.

Với p = 2 ta có $2^9 = 512$, $2^{10} = 1024$ nên k = 9 và

$$\alpha_2 = \sum_{i=1}^{9} \left[\frac{1000}{2^i}\right] = 500 + 250 + 125 + 62 + 31 + 15 + \\ + 7 + 3 + 1 = 994$$

với p = 5 ta có $5^4 = 625, 5^5 = 3125$ nên k = 4 và

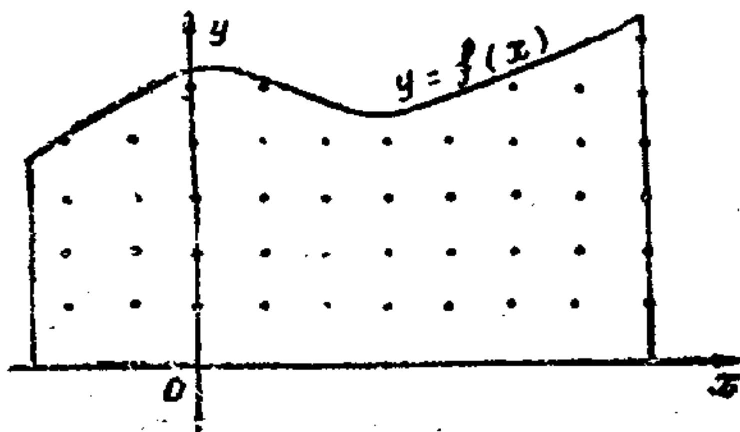
$$\alpha_5 = \sum_{i=1}^{4} \left[\frac{1000}{5^i}\right] = 200 + 40 + 8 + 1 = 249.$$

Từ đó ta có thể suy ra $2^{994} \mid 1000!$ nhưng 2^{995} không chia hết 1000 ! cũng như vậy $5^{249} \mid 1000!$ nhưng 5^{250} không chia hết 1000! Hơn nữa vì 10 = 2.5 và (2,5) = 1 nên có thể nói rằng số 1000! trong hệ ghi số thập phân tận cùng bên phải có 249 chữ số 0.

III — ĐIỂM NGUYÊN. Trong mặt phẳng tọa độ ta gọi điểm có tọa độ là những số nguyên là điểm nguyên. Ta có kết quả hiển nhiên sau đây nói lên quan hệ giữa các điểm nguyên trong mặt phẳng tọa độ với hàm số phần nguyên.

Giả sử hàm số f(x) liên tục và không âm trên đoạn [a ; b]. Số các điểm nguyên trong miền xác định bởi

$$a \leqslant x \leqslant b,\ 0 < y \leqslant f(x),$$



(nghĩa là không kể các điểm nguyên nằm trên trục hoành) bằng :

$$\sum_{a \leqslant k \leqslant b} [f(k)],$$

trong đó k lấy các giá trị nguyên thuộc đoạn [a, b].

§ 2. SỐ CÁC ƯỚC CỦA MỘT SỐ TỰ NHIÊN

I – ĐỊNH NGHĨA. Cho số tự nhiên n khác không. Ta gọi $\tau(n)$ là số các ước tự nhiên của n.

Để cho gọn ta viết

$$\tau(n) = \sum_{d \mid n} 1$$

II – CÁCH TÍNH

1. Với $n = 1$ ta có $\tau(1) = 1$

2. Với $n = p^{\alpha}$, trong đó p là một số nguyên tố và α là một số tự nhiên khác 0, ta có

$$\tau(p^{\alpha}) = \alpha + 1.$$

Thật vậy các ước của p^{α} là và chỉ là các số 1, p, $p^2, \ldots, p^{\alpha}$.

3. Trong trường hợp tổng quát $n = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_k^{\alpha_k}$ là dạng phân tích tiêu chuẩn của số tự nhiên $n > 1$, ta có công thức

$$\tau(n) = (\alpha_1 + 1)(\alpha_2 + 1) \ldots (\alpha_k + 1). \qquad (1)$$

Chứng minh. Để chứng minh công thức (1), trước tiên ta có nhận xét :

Với hai số tự nhiên khác không a và b nguyên tố cùng nhau thì ta có $\tau(ab) = \tau(a)\,\tau(b)$.

Thật vậy, giả sử $x_1, x_2, \ldots, x_{\tau(a)}$ là những ước của a và $y_1, y_2, \ldots, y_{\tau(b)}$ là những ước của b, theo chú ý 1.c) IV, § 1 bài thứ hai, các ước của tích ab là và chỉ là các số

$$d_{ij} = x_i y_j \; (i = 1, 2, \ldots, \tau(a) ; \; j = 1, 2, \ldots, \tau(b))$$

Có tất cả $\tau(a).\tau(b)$ số d_{ij} như vậy, nên ta có

$$\tau(ab) = \tau(a)\,\tau(b).$$

Bây giờ ta chứng minh công thức (1) bằng phép qui nạp toán học theo k.

Với k = 1 công thức đúng vì ta đã có $\tau(p^\alpha) = \alpha + 1$.

Giả sử công thức (1) đã đúng với mọi số tự nhiên có k – 1 ước nguyên tố, ta phải chứng minh công thức (1) cũng đúng với các số tự nhiên có k ước nguyên tố. Giả sử $n = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_k^{\alpha_k}$ là dạng phân tích tiêu chuẩn của n, nghĩa là $p_1, p_2, \ldots, p_k$ là các số nguyên tố khác nhau, vì vậy :

$(p_1 \cdot p_2 \ldots p_{k-1}, p_k) = 1$, theo nhận xét ở trên ta có

$$\tau(n) = \tau(p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_{k-1}^{\alpha_{k-1}})\ \tau(p_k^{\alpha_k})$$

và theo giả thiết qui nạp ta được

$$\tau(n) = (\alpha_1 + 1)\ (\alpha_2 + 1) \ldots (\alpha_{k-1} + 1)\ (\alpha_k + 1)$$

Đến đây công thức (2) được chứng minh.

Ví dụ : $n = 360 = 2^3 3^2 5$ ta có $\tau(360) = 4.3.2. = 24$

III – CHÚ Ý.

1) Theo định nghĩa, $\tau(n)$ biểu thị số các ước dương của n, nó còn biểu thị số các nghiệm nguyên dương của phương trình $x_1 x_2 = n$, trong đó các nghiệm sai khác về thứ tự giá trị các ẩn cũng được coi là khác nhau.

Với ý nghĩa đó ta cũng có thể mở rộng khái niệm hàm số $\tau(m)$ thành hàm số $\tau_k(m)$ $(k \geqslant 2)$ biểu thị số các nghiệm nguyên dương của phương trình $x_1 . x_2 \ldots x_k = m$, trong đó cũng như trên, các nghiệm sai khác về thứ tự giá trị của các ẩn được coi là khác nhau. Như vậy $\tau(m) = \tau_2(m)$ là một trường hợp đặc biệt của hàm số $\tau_k(m)$.

2. Như nhận xét ở trên, nếu có hai số tự nhiên a và b mà $(a, b) = 1$ thì $\tau(a \cdot b) = \tau(a) \cdot \tau(b)$, bởi lý do ấy ta nói hàm số $\tau(n)$ có tính chất nhân. Để đi đến định nghĩa hàm số có tính chất nhân ta hãy định nghĩa khái niệm hàm số số học.

Ta gọi là *hàm số số học*, một hàm số mà miền xác định của nó là một bộ phận của tập hợp số tự nhiên.

Một hàm số số học $\theta(n)$ gọi là *có tính chất nhân* nếu như nó thỏa mãn các điều kiện sau đây :

1. $\theta(n)$ xác định với mọi giá trị tự nhiên khác không của n và là khác không với ít nhất một giá trị nào đó của n.

2. Với hai số tự nhiên n_1, n_2 tùy ý nguyên tố cùng nhau thì $\theta(n_1 n_2) = \theta(n_1)\ \theta(n_2)$.

Trong trường hợp điều kiện 2) được thỏa mãn với mọi cặp số tự nhiên n_1, n_2 (nguyên tố cùng nhau hay không nguyên tố cùng nhau) thì ta nói hàm số $\theta(n)$ *có tính chất nhân hoàn toàn*.

Hai hàm số chúng ta sẽ nghiên cứu ở dưới đây cũng là những hàm số có tính chất nhân.

§ 3. TỔNG CÁC ƯỚC CỦA MỘT SỐ TỰ NHIÊN

I – ĐỊNH NGHĨA. Cho số tự nhiên n khác không. Ta gọi $\sigma(n)$ là tổng các ước tự nhiên của n

Để cho gọn ta viết :

$$\sigma(n) = \sum_{d/n} d.$$

II – CÁCH TÍNH

1. Với $n = 1$ ta có $\sigma(1) = 1$

2. Với $n = p^{\alpha}$, trong đó p là một số nguyên tố và là một số tự nhiên kkác 0, ta có

$$\sigma(p^{\alpha}) = 1 + p + p^2 + \dots + p^{\alpha} = \frac{p^{\alpha+1} - 1}{p - 1}.$$

3. Giả sử $n = p_1^{\alpha_1} \dots p_k^{\alpha_k}$ là dạng phân tích tiêu chuẩn của số tự nhiên $n > 1$, ta có công thức

$$\sigma(n) = \frac{p_1^{\alpha_1+1}}{p_1 - 1} \cdot \frac{p_2^{\alpha_2+1}}{p_2 - 1} \dots \frac{p_k^{\alpha_k+1}}{p_k - 1}$$

Chứng minh. Trước hết ta nhận thấy rằng với hai số tự nhiên khác không a và b nguyên tố cùng nhau thì $\sigma(ab) = \sigma(a)\sigma(b)$.

Thật vậy, giả sử $x_1, x_2, \dots x_{\tau(a)}$ là những ước tự nhiên của a và $y_1, y_2, \dots, y_{\tau(y)}$ là những ước tự nhiên của b, ta có ước của tích ab là và chỉ là các số:

$d_{ij} = x_i \cdot y_j$ ($i = 1, 2, \dots \tau(a)$, $j = 1, 2, \dots \tau(b)$) nên ta được

$$\sigma(ab) = \sum_{d/ab} d = \sum_{\substack{i = 1, 2, \dots, \tau(a) \\ j = 1, 2, \dots \tau(b)}} x_i y_j = \sum_{i=1}^{\tau(a)} x_i \sum_{j=1}^{\tau(b)} y_j = \sigma(a)\sigma(b)$$

Bây giờ ta chứng minh công thức (2) bằng phép qui nạp toán học theo k.

Với $n = p^{\alpha}$ ta có $\sigma(p^{\alpha}) = \dfrac{p^{\alpha+1} - 1}{p - 1}$ nên công thức (2) đúng với $k = 1$.

Giả sử công thức (2) đã đúng với mọi số tự nhiên có $k-1$ $(k-1>1)$ ước nguyên tố, ta phải chứng minh công thức (2) cũng đúng với các số tự nhiên có k ước nguyên tố. Giả sử $n = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_k^{\alpha_k}$ là dạng phân tích tiêu chuẩn của n, nghĩa là $p_1, p_2, \ldots, p_k$ là các số nguyên tố khác nhau nên $(p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_{k-1}^{\alpha_{k-1}}, p_k) = 1$. theo nhận xét ở trên ta có:

$$\sigma(n) = \sigma(p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_{k-1}^{\alpha_{k-1}}).\sigma(p_k^{\alpha_k})$$

Và theo giả thiết qui nạp ta được

$$\sigma(n) = \frac{p_1^{\alpha_1+1}-1}{p_1-1} \cdot \frac{p_2^{\alpha_2+1}-1}{p_2-1} \ldots \frac{p_{k-1}^{\alpha_{k-1}+1}-1}{p_{k-1}-1} \cdot \frac{p_k^{\alpha_k+1}-1}{p_k-1}$$

Đến đây công thức (2) được chứng minh.

Ví dụ: $n = 360 = 2^3 . 3^2 . 5$ ta có

$$\sigma(360) = \frac{2^4-1}{2-1} \cdot \frac{3^3-1}{3-1} \cdot \frac{5^2-1}{5-1} = 1170$$

III – SỐ HOÀN CHỈNH

1. Định nghĩa. Số tự nhiên n khác 0 được gọi là *số hoàn chỉnh* nếu $\sigma(n) = 2n$.

Ví dụ: n = 6 là một số hoàn chỉnh bởi vì

$$\sigma(6) = 1 + 2 + 3 + 6 = 2 . 6.$$

Nếu trong các ước tự nhiên của n ta không kể đến chính nó thì số hoàn chỉnh bằng tổng các ước của nó.

2. Định lý. *Điều kiện cần và đủ để cho số chẵn n là một số hoàn chỉnh là nó có dạng*

$$n = 2^{k-1}(2^k - 1),$$

trong đó $k \geqslant 2$ và $p = 2^k - 1$ là một số nguyên tố.

Chứng minh. a) *Điều kiện đủ.* Giả sử $n = 2^{k-1}(2^k - 1)$ trong đó $k \geqslant 2$ và $p = 2^k - 1$ là một số nguyên tố. Khi ấy $(p, 2) = 1$ nên $2^{k-1} \cdot p$ là dạng phân tích tiêu chuẩn của n, do đó

$\sigma(n) = \sigma(2^{k-1})\,\sigma(p) = (2^k - 1)(1 + p) = 2^k(2^k - 1)$

hay

$$\sigma(n) = 2 \cdot 2^{k-1}(2^k - 1) = 2.n$$

nghĩa là n là số hoàn chỉnh.

b) *Điều kiện cần.* Giả sử n là một số hoàn chỉnh chẵn, gọi lũy thừa của 2 trong dạng phân tích tiêu chuẩn của n là 2^{k-1}, dĩ nhiên $k \geqslant 2$ và ta có $n = 2^{k-1} b$, trong đó b là một số lẻ. Khi ấy $(2^{k-1}, b) = 1$ nên

$$\sigma(n) = \sigma(2^{k-1})\,\sigma(b) = (2^k - 1)\,\sigma(b),$$

theo giả thiết n là số hoàn chỉnh vậy ta có

$$\sigma(n) = 2n = 2^k b$$

do đó ta được

$$(2^k - 1)\,\sigma(b) = 2^k \cdot b$$

Đẳng thức này cho ta $2^k - 1 \mid 2^k b$, nhưng vì $(2^{k-1}, 2^k) = 1$ nên ta suy ra $2^k - 1 \mid b$, nghĩa là ắt có số tự nhiên c (dĩ nhiên $c < b$) sao cho

$$b = (2^k - 1)\,c.$$

Thay giá trị này vào đẳng thức vừa có ở trên ta được

$$(2^k - 1)\,\sigma(b) = 2^k(2^k - 1)\,c$$

cho nên

$$\sigma(b) = 2^k c = (2^k - 1)\,c + c$$

hay là

$$\sigma(b) = b + c$$

Ta sẽ chứng tỏ b phải là nguyên tố và do đó $c = 1$. Thật vậy, nếu không như thế thì do $b > 1$ nên b phải có ít nhất ba ước tự nhiên, nghĩa là ngoài các ước là

b, c, nó còn có ít nhất một ước khác nữa, do đó lại sẽ có $\sigma(b) > b+c$, vô lí. Vậy b là số nguyên tố, suy ra c = 1, cho nên ta được

$$n = 2^{k-1}(2^k - 1)$$

trong đó $k > 2$ và $2^k - 1$ là một số nguyên tố. Định lý được chứng minh.

3. Như ta đã biết nếu $b = 2^k - 1$ là số nguyên tố thì k cũng là số nguyên tố và b chính là số nguyên tố Mécxen. Vậy mỗi số nguyên tố Mécxen cho ta một số hoàn chỉnh chẵn và các số hoàn chỉnh chẵn là:

$$2^{p-1}(2^p - 1)$$

với p và $2^p - 1$ đều là nguyên tố.

Bài toán về số hoàn chỉnh chẵn liên quan mật thiết với bài toán về số nguyên tố Mecxen. Người ta chưa biết được tập hợp số nguyên tố Mecxen là hữu hạn hay vô hạn cho nên cũng chưa biết tập hợp các số hoàn chỉnh chẵn là hữu hạn hay vô hạn. Cho đến năm 1971 người ta tìm được 24 số nguyên tố Mecxen và như vậy có tương ứng 24 số hoàn chỉnh chẵn, số hoàn chỉnh chẵn lớn nhất thứ 24 do nhà toán học Takiman tìm được hồi tháng 6 năm 1971, đó là $2^{19936}(2^{19937} - 1)$ gồm 12003 chữ số trong hệ ghi số thập phân. Số này được tính ra sau 40 phút trên một loại máy tính điện tử liên hợp hiện đại. Năm 1979 D.SLovinski phát hiện số hoàn chỉnh thứ 27 là $2^{44496}(2^{44497} - 1)$ và tiếp đó, năm 1983 ông lại phát hiện số hoàn chỉnh $2^{86242}(2^{86243} - 1)$ tuy nhiên chưa biết đó có phải là số hoàn chỉnh thứ 28 hay không vì chưa biết số nguyên tố Mecxen M_{86243} có phải là số nguyên tố Mecxen thứ 28 hay không.

Cho đến nay người ta chưa biết một số hoàn chỉnh lẻ nào và bài toán có hay không các số hoàn chỉnh lẻ là một bài toán chưa được giải quyết. Cũng có giả thuyết cho rằng không có số hoàn chỉnh lẻ.

§ 4. HÀM SỐ ƠLE $\varphi(n)$

I – ĐỊNH NGHĨA. Cho số tự nhiên n khác không. Ta gọi $\varphi(n)$ là số các số tự nhiên nhỏ hơn n và nguyên tố với n.

Ví dụ: $\varphi(1) = 1$, $\varphi(2) = 1$, $\varphi(3) = 2$, $\varphi(11) = 10$, $\varphi(12) = 4$.

Để cho gọn ta viết

$$\varphi(n) = \sum_{\substack{0 \leqslant k \leqslant n-1 \\ (k,\, n) = 1}} 1$$

Ta chú ý rằng với mỗi số tự nhiên n ta có $(n, n) = (n, 0) = n$ nên số các số tự nhiên khác không, không vượt quá n và nguyên tố với n cũng bằng $\varphi(n)$, nghĩa là ta còn có

$$\varphi(n) = \sum_{\substack{1 \leqslant k \leqslant n \\ (k,\, n) = 1}} 1$$

II – CÁCH TÍNH

1. Với $n = 1$ ta có $\varphi(1) = 1$.

2. Với $n = p^{\alpha}$ trong đó p là một số nguyên tố và α là một số tự nhiên khác không, ta có

$$\varphi(p^{\alpha}) = p^{\alpha} - p^{\alpha-1} = p^{\alpha-1}(p-1) = p^{\alpha}\left(1 - \frac{1}{p}\right).$$

Thật vậy, bởi vì p là nguyên tố nên hoặc $(k, p) = 1$ hoặc $k \vdots p$, do đó ta có

$$\varphi(p^{\alpha}) = \sum_{\substack{1 \leqslant k \leqslant p^{\alpha} \\ (k,\, p) = 1}} 1 = p^{\alpha} - \sum_{\substack{1 \leqslant k \leqslant p^{\alpha} \\ k \,\vdots\, p}} 1 = p^{\alpha} - \left[\frac{p^{\alpha}}{p}\right] = p^{\alpha} - p^{\alpha-1}.$$

3. Giả sử $n = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_k^{\alpha_k}$ là dạng phân tích tiêu

chuẩn của số tự nhiên $n > 1$. ta có công thức

$$\varphi(n) = n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\cdots\left(1 - \frac{1}{p_k}\right). \qquad (3)$$

Chứng minh. Để chứng minh công thức (3), trước hết ta chứng minh một vài mệnh đề phụ sau đây:

a) *Giả sử a và b là hai số tự nhiên khác 0, nguyên tố cùng nhau, khi ấy với mỗi số tự nhiên y cho trước, thì trong b số $ax + y (x = 0, 1, ..., b - 1)$ có $\varphi(b)$ số nguyên tố với b.*

Thật vậy, giả sử r_x là số dư trong phép chia $ax + y$ cho b, như vậy thì $ax + y$ nguyên tố với b khi và chỉ khi r_x nguyên tố với b.

Bây giờ ta chia b số $ax+y$ cho b, ta được b số dư $r_0, r_1, ..., r_{b-1}$ thỏa mãn $0 \leqslant r_x < b$ $(x = 0, 1, ..., b-1)$. b số dư này đôi một khác nhau bởi vì nếu không thế thì ắt có $r_i = r_j$, $i \neq j$, $0 \leqslant i, j < b$ ta suy ra từ đó rằng $ai + r_i - (aj + r_j) = a(i - j)$ chia hết cho b với $0 < |i - j| < b$ và $(a, b) = 1$, điều này không thể có được.

Như vậy ta có đẳng thức tập hợp

$$\{r_0, r_1, ..., r_{b-1}\} = \{0, 1, ..., b - 1\}.$$

Dựa vào chú ý ở trên thì ta có kết quả là số các số trong tập hợp $\{ax + y \mid x = 0, 1, ..., b - 1\}$ mà nguyên tố với b bằng số các số trong tập hợp $\{0, 1, ..., b - 1\}$ mà nguyên tố với b, số đó chính bằng $\varphi(b)$.

b) *Với hai số tự nhiên khác không a và b nguyên tố cùng nhau, ta có $\varphi(ab) = \varphi(a)\,\varphi(b)$.*

Thật vậy, nếu trong hai số a và b có một số bằng 1 thì hiển nhiên $\varphi(ab) = \varphi(a)\,\varphi(b)$ vì $\varphi(1) = 1$.

Bây giờ giả sử $a > 1$, $b > 1$ ta lập bảng gồm ab số tự nhiên từ 0 đến $ab - 1$ như sau

$$M = \begin{bmatrix} 0 & 1 & \ldots & a-1 \\ a & a+1 & \ldots & a+(a-1) \\ 2a & 2a+1 & \ldots & 2a+(a-1) \\ \ldots & \ldots & \ldots & \ldots \\ (b-1)a & (b-1)a+1 & \ldots & (b-1)a+(a-1) \end{bmatrix}$$

Dễ dàng thấy rằng một số trong bảng là nguyên tố với tích ab khi và chỉ khi số đó nguyên tố với cả a và b. Do đó để tìm các số nguyên tố với tích ab trước hết ta tìm các số nguyên tố với a rồi trong các số đó ta xem những số nào nguyên tố với b.

Các số ở trong bảng M có dạng $ax + y$, trong đó $x = 0, 1, \ldots, b-1$; $y = 0, 1, \ldots, a-1$.

Rõ ràng là $(ax + y, a) = (y, a)$ cho nên các số trong bảng nguyên tố với a khi và chỉ khi nó ở cột thứ y nào đó mà $(y, a) = 1$, như vậy có $\varphi(a)$ cột như thế. Trong mỗi cột y ta có b số dạng $ax + y$, $x = 0, 1, \ldots, b-1$, theo mệnh đề a) thì trong b số đó có tất cả $\varphi(b)$ số nguyên tố với b. Vậy trong bảng M có tất cả $\varphi(a)\,\varphi(b)$ số nguyên tố với tích ab. Nhưng ta đã biết, theo định nghĩa, số các số trong bảng M nguyên tố với tích ab là $\varphi(ab)$, do đó ta có

$$\varphi(ab) = \varphi(a)\,\varphi(b).$$

c) Bây giờ ta chứng minh công thức (3) bằng phép qui nạp toán học theo k.

Với $n = p^{\alpha}$ ta có $\varphi(p^{\alpha}) = p^{\alpha}\left(1 - \frac{1}{p}\right)$ nên công thức (3) đúng với $k = 1$.

Giả sử công thức (3) đã đúng với mọi số tự nhiên có $k-1$ ước nguyên tố ($k - 1 \geqslant 1$), ta phải chứng minh công thức (3) cũng đúng với các số tự nhiên có k ước nguyên tố. Giả sử $n = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_k^{\alpha_k}$ là dạng phân tích

tiêu chuẩn của n, vì $p_1, p_2, \ldots, p_k$ là những số nguyên tố khác nhau nên

$$(p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_{k-1}^{\alpha_{k-1}}, p_k^{\alpha_k}) = 1.$$

Theo nhận xét ở trên thì

$$\varphi(n) = \varphi(p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_{k-1}^{\alpha_{k-1}}) \varphi(p_k^{\alpha_k})$$

và theo giả thiết qui nạp ta được

$$\varphi(n) = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_{k-1}^{\alpha_{k-1}} \left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right) \ldots$$

$$\ldots \left(1 - \frac{1}{p_{k-1}}\right) p_k^{\alpha_k} \left(1 - \frac{1}{p_k}\right)$$

hay là

$$\varphi(n) = n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right) \ldots \left(1 - \frac{1}{p_k}\right).$$

Đến đây công thức (3) được chứng minh hoàn toàn.

Ví dụ: $n = 360 = 2^3 . 3^2 . 5$ ta có

$$\varphi(360) = 360\left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{3}\right)\left(1 - \frac{1}{5}\right) =$$

$$= 360 . \frac{1}{2} . \frac{2}{3} . \frac{4}{5} = 96.$$

BÀI TẬP

3.1. a) Chứng minh rằng với x là số thực không nguyên ta có

$$[-x] = -[x] - 1.$$

b) Chứng minh rằng với x và y là những số thực không nguyên mà $x + y = a$ là một số nguyên thì ta có

$$[x] + [y] = a - 1.$$

3.2. a) Chứng minh rằng với m là một số nguyên và x là một số thực tùy ý ta có

$$[x + m] = [x] + m.$$

b) Chứng minh rằng với n là một số tự nhiên ta có

$$\left[\frac{n}{2}\right] + \left[\frac{n+1}{2}\right] = n.$$

3.3. Chứng minh rằng:

a) Với mọi số thực x và y ta có

$$[x]+[y] \leqslant [x+y] \leqslant [x]+[y]+1.$$

Đặc biệt

$$2[x] \leqslant [2x] \leqslant 2[x]+1.$$

b) Với mọi số thực $x_1, x_2, \ldots, x_n$ ta có

$$[x_1]+[x_2]+\ldots+[x_n] \leqslant [x_1+x_2+\ldots+x_n].$$

Đặc biệt: $n[x] \leqslant [nx]$.

c) Với mọi số thực x và y ta có

$$[2x]+[2y] \geqslant [x]+[y]+[x+y].$$

3.4. Chứng minh rằng

a) Với $0 \leqslant \alpha < 1$ ta có $[\alpha]+\left[\alpha+\frac{1}{2}\right]=[2\alpha]$.

b) Với x là một số thực tùy ý ta có

$$[x]+\left[x+\frac{1}{2}\right]=[2x].$$

c) Với x là một số thực tùy ý và n là một số nguyên dương ta có

$$[x]+\left[x+\frac{1}{n}\right]+\ldots+\left[x+\frac{n-1}{n}\right]=[nx].$$

3.5. Chứng minh rằng

a) Nếu $m \geqslant 2$ và $n \geqslant 2$, $(m, n)=1$ thì ta có

$$\left[\frac{m}{n}\right]+\left[\frac{2m}{n}\right]+\ldots+\left[\frac{(n-1)m}{n}\right]=\left[\frac{(m-1)(n-1)}{2}\right].$$

b) Với p, q là những số tự nhiên lẻ và $(p, q)=1$ ta có

$$\left[\frac{q}{p}\right]+\left[\frac{2q}{p}\right]+\ldots+\left[\frac{p'q}{p}\right]+\left[\frac{p}{q}\right]+$$
$$+\left[\frac{2p}{q}\right]+\ldots+\left[\frac{q'p}{q}\right]=p'q'.$$

trong đó $p'=\frac{p-1}{2}$, $q'=\frac{q-1}{2}$.

3.6. Cho p là một số nguyên tố và α là một số nguyên dương. Chứng minh rằng tích.

$$(\alpha+1)(\alpha+2)\ldots(p^{\alpha}-1)p^{\alpha}$$

chia hết cho p^{α} và không chia hết cho $p^{\alpha+1}$.

3.7. a) Chứng minh rằng $[(2+\sqrt{3})^n]$ là một số lẻ (với n là một số tự nhiên cho trước).

b) Tìm số mũ của 2 trong dạng phân tích tiêu chuẩn của $[(1+\sqrt{3})^n]$ (với n là một số tự nhiên khác 0).

3.8. Chứng minh rằng:

a) Với mỗi số nguyên dương n cho trước ta có

$$\frac{(2n)!\,6}{n!\,(n+2)!}$$

là một số nguyên ;

b) Với m và n là những số nguyên không âm cho trước ta có

$$\frac{(2m)!\,(2n)!}{m!\,n!\,(m+n)!}$$

là một số nguyên.

Ta qui ước $0! = 1$).

(Thi vô địch toán quốc tế – 1972)

3.9. Cho a, m là những số nguyên dương và $(a, m) = 1$ Chứng minh rằng

$$\sum_{x=1}^{m}\left\{\frac{ax+b}{m}\right\}=\frac{m-1}{2}.$$

3.10. Tìm tổng

$$\left[\frac{n+1}{2}\right]+\left[\frac{n+2}{2^2}\right]+\ldots+\left[\frac{n+2^k}{2^{k+1}}\right]+\ldots,$$

trong đó n là một số tự nhiên cho trước.

(Thi vô địch toán quốc tế – 1968)

3.11. Tìm tất cả các số tự nhiên n

a) biết dạng phân tích tiêu chuẩn $p^{\alpha}q^{\beta}$ và $\tau(n)=6$, $\sigma(n)=28$.

b) biết dạng phân tích tiêu chuẩn $n=2^{\alpha}3^{\beta}$ và $\sigma(n)=403$,

c) biết dạng phân tích tiêu chuẩn $n=3p^2$ và $\sigma(n)=124$;

d) biết dạng phân tích tiêu chuẩn $n=3^{\alpha}5^{\beta}7^{\gamma}$ và $\varphi(n)=3600$;

e) biết dạng phân tích tiêu chuẩn $n=2^{\alpha}3^{\beta}p$ và $\varphi(n)=180$.

3.12. a) Chứng minh rằng điều kiện cần và đủ để $\tau(n)$ là một số lẻ là n phải có dạng $n = a^2$.

b) Chứng minh rằng điều kiện cần và đủ để $\sigma(n)$ là một số lẻ là n phải có dạng $n = a^2$ hoặc $n = 2b^2$.

c) Chứng minh rằng với $n > 2$ ta có $\varphi(n)$ là một số chẵn. Hãy tìm tất cả các số nguyên dương n sao cho $\varphi(n)$ không là bội của 4.

3.13. Tìm công thức tính cho

$$\sigma_k(n) = \sum_{d/n} d^k$$

theo $n = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_k^{\alpha_k}$.

3.14. Chứng minh các đẳng thức

a) $\prod_{d|n} d = n^{(1/2)\tau(n)}$; b) $\sum_{d|n} d = n \sum_{d|n} \frac{1}{d}$,

3.15. Chứng minh rằng

$$\text{a)} \quad \sum_{k=1}^{n} \tau(k) = \sum_{k=1}^{n} \left[\frac{n}{k}\right];$$

$$\text{b)} \quad \sum_{k=1}^{n} \sigma(k) = \sum_{k=1}^{n} k\left[\frac{n}{k}\right].$$

3.16 a) Tìm các số hoàn chỉnh nếu biết dạng phân tích tiêu chuẩn của nó là một trong các dạng sau

$$n = pq\ ;\ n = p^2 q.$$

b) Chứng minh rằng không tồn tại số hoàn chỉnh mà phân tích tiêu chuẩn của nó là một trong các dạng sau

$$n = p^\alpha\ ;\ n = p^3 . q.$$

3.17. Số tự nhiên $n \geqslant 1$ được gọi là số thiếu nếu $\sigma(n) < 2n$, được gọi là số thừa nếu $\sigma(n) > 2n$. Chứng minh rằng

a) lũy thừa của một số nguyên tố là một số thiếu;

b) có vô số số tự nhiên n thỏa mãn $\sigma(n) = 2n - 1$;

c) số lẻ chỉ có hai ước nguyên tố khác nhau là số thiếu.

3.18 Chứng minh rằng

a) nếu $m \mid n$ thì $\varphi(m) \mid \varphi(n)$;

b) $\varphi(m^{n}) = m^{n-1} \varphi(m)$.

3.19 Chứng minh rằng

a) $\sum_{i=0}^{\alpha} \varphi(p^{i}) = p^{\alpha}$; b) $\sum_{d|n} \varphi(d) = n$.

3.20. Chứng minh rằng với $m > 2$ ta có $\varphi(m) > 1$ Dựa vào kết quả đó chứng minh rằng có vô số số nguyên tố.

3.21. Gọi $m = [a, b]$, $d = (a, b)$, chứng minh rằng

a) $(ab) = d\,\varphi(m)$

b) $\varphi(a).\ \varphi(b) = \varphi(m)\ \varphi(d)$

c) $\varphi(ab)\ \varphi(d) = d\ \varphi(a).\ \varphi(b)$.

3.22. Chứng minh rằng $\varphi(x) = 2^{s}$ khi và chỉ khi $x = 2^{s+1}$ hoặc $x = 2^{n} p_1 p_2 \ldots p_k$, trong đó $p_1, p_2, \ldots, p_k$ là những số nguyên tố Phécma khác nhau.

3.23. Tìm tất cả các số tự nhiên x sao cho

a) $\varphi(x) = 2^{5}$; b) $\varphi(x) = 12$.

BÀI THỨ TƯ

LIÊN PHÂN SỐ

§ 1. ĐỊNH NGHĨA LIÊN PHÂN SỐ

I – ĐỊNH NGHĨA. Cho một số hữu tỉ $\frac{a}{b}$, trong đó a, b là những số nguyên, $b > 0$. Thực hiện thuật toán Ơclid trên hai số a,b, giả sử ta được

$$a = bq_0 + r_1,\ 0 < r_1 < b,$$
$$b = r_1 q_1 + r_2,\ 0 < r_2 < r_1,$$
$$\cdots\cdots\cdots$$

$$r_{n-2} = r_{n-1} q_{n-1} + r_n \; . \; 0 < r_n < r_{n-1},$$
$$r_{n-1} = r_n q_n \quad (q_n > 1).$$

Từ đó để biểu diễn số hữu tỉ $\frac{a}{b}$ ta có thể viết

$$\frac{a}{b} = q_o + \cfrac{1}{\cfrac{b}{r_1}} = q_o + \cfrac{1}{q_1 + \cfrac{1}{\cfrac{r_1}{r_2}}} = \ldots$$

cuối cùng ta được

$$\frac{a}{b} = q_o + \cfrac{1}{q_1 + \cfrac{1}{q_2 + \cdot \cdot + \cfrac{1}{q_n}}} \qquad (1)$$

Biểu thức (1) gọi là một *liên phân số hữu hạn cấp n*. Vậy liên phân số hữu hạn cấp n là một biểu thức có dạng

$$q_o + \cfrac{1}{q_1 + \cfrac{1}{q_2 + \cdot \cdot + \cfrac{1}{q_n}}}, \qquad (1)$$

trong đó q_o là một số nguyên tùy ý, $q_1, q_2, \ldots, q_n$ là những số nguyên dương và $q_n > 1$. Số q_s gọi là *số hạng thứ s hay là thương hụt thứ s* của liên phân số (1). Để cho gọn, ta ký hiệu liên phân số (1) dưới dạng

$$[q_o \; ; \; q_1, \; q_2 \; , \ldots, \; q_n].$$

Ví dụ : Dựa vào kết quả của thuật toán Ơclit thực hiện trên hai số 924 và 360 ở bài thứ nhất ta có

$$\frac{924}{360} = 2 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{3 + \cfrac{1}{4}}}} = [2 : 1, 1, 3, 4]$$

II. HỆ QUẢ. Mọi số hữu tỷ đều có thể biểu diễn được dưới dạng một liên phân số hữu hạn, ngược lại mỗi liên phân số hữu hạn đều biểu thị một số hữu tỷ hay nói cách khác, đều có giá trị là một số hữu tỷ. Ta có thể tính được giá trị này bằng cách thực hiện các phép tính hữu tỷ về phân số trong biểu thức liên phân số bắt đầu từ dưới trở lên.

III – TÍNH DUY NHẤT CỦA CÁCH BIỂU DIỄN MỘT SỐ HỮU TỶ THÀNH LIÊN PHÂN SỐ.

1. *Nhận xét*. a) Cho liên phân số $[q_0; q_1, q_2, \ldots, q_n]$. Khi ấy biểu thức

$$q_k + \cfrac{1}{q_{k+1} + \cdots + \cfrac{1}{q_n}} \qquad (0 \leqslant k \leqslant n)$$

cũng là một liên phân số hữu hạn, bởi vì $q_{k+1}, \ldots, q_n$ là những số nguyên dương và $q_n > 1$.

b) Phần nguyên của số hữu tỉ biểu diễn bởi liên phân số $[q_0; q_1, q_2, \ldots, q_n]$ bằng thương hụt đầu tiên q_0 của nó.

Thật vậy, nếu $n = 0$ thì kết quả là hiển nhiên, bởi vì lúc này q_0 là một số nguyên, liên phân số chỉ có một số hạng $[q_0] = q_0$.

Nếu $n = 1$ thì

$$[q_0; q_1] = q_0 + \frac{1}{q_1}, \; q_1 > 1$$

cho nên phần nguyên của số hữu tỉ biểu diễn bởi $[q_0; q_1]$ bằng q_0 vì $0 < \frac{1}{q_1} < 1$.

Nếu $n > 1$ thì

$$[q_0; q_1, q_2, \ldots, q_n] = q_0 + \cfrac{1}{q_1 + \cfrac{1}{q_2 + \ddots + \cfrac{1}{q_n}}}$$

ở đó $0 < \cfrac{1}{q_1 + \cfrac{1}{q_2 + \ddots + \cfrac{1}{q_n}}} < 1$ vì $q_1 \geqslant 1$, bởi vậy phần nguyên của số hữu tỉ biểu diễn bởi $[q_0; q_1, q_2, \ldots, q_n]$ bằng q_0

2. *Mỗi số hữu tỉ $\frac{a}{b}$ với $b > 0$ chỉ có một cách duy nhất biểu diễn thành liên phân số.*

Chứng minh. Giả sử $\frac{a}{b}$ có hai cách biểu diễn thành liên phân số

$$[q_0; q_1, \ldots, q_n] \text{ và } [q'_0; q'_1, \ldots, q'_{n'}]$$

trong đó $q_n > 1$, $q'_{n'} > 1$.

Ta sẽ chứng minh $n' = n$ và $q'_i = q_i$, $i = 0, 1, \ldots, n$. Thật vậy, theo nhận xét ở trên ta có:

$$\left[\frac{a}{b}\right] = q_0 = q'_0$$

cho nên từ $\frac{a}{b} = [q_0; q_1, \ldots, q_n] = [q'_0; q'_1, \ldots, q'_{n'}]$ ta còn có

$$[q_1; q_2, \ldots, q_n] = [q'_1; q'_2, \ldots, q'_{n'}].$$

Lại theo nhận xét ở trên ta có

$$q_1 = q'_1$$

và

$$[q_2 ; q_3, \dots, q_n] = [q'_2 : q'_3, \dots, q'_{n'}]$$

Cứ tiếp tục làm như vậy ta được

$$q_o = q'_o , \; q_1 = q'_1 , \; q_2 = q'_2 , \dots$$

Nếu $n \neq n'$ thì ta sẽ có

$$0 = \cfrac{1}{q'_{n'+1} + \cdots + \cfrac{1}{q'_{n'}}}$$

$$\text{hoặc } \cfrac{1}{q'_{n+1} + \cdots + \cfrac{1}{q_n}} = 0$$

là điều không thể được.

Bởi vậy $n = n'$ và cuối cùng ta được

$$q_o = q'_o , \; q_1 = q'_1 , \; q_2 = q'_2 , \dots, \; q_n = q'_n .$$

Định lý được chứng minh.

§2. GIẢN PHÂN

I - ĐỊNH NGHĨA. Cho liên phân số

$$q_o + \cfrac{1}{q_1 + \cfrac{1}{q_2 + \cdots + \cfrac{1}{q_n}}} . \qquad (1)$$

Ta gọi *giản phân cấp s* (hay *giản phân thứ s*) với $0 \leqslant s < n$ của liên phân số (1) là phân số $\delta_s = \dfrac{P_s}{Q_s}$ được xác định như sau:

$$\begin{cases} P_0 = q_0, \\ Q_0 = 1; \end{cases} \qquad \begin{cases} P_1 = q_1 q_0 + 1, \\ Q_1 = q_1; \end{cases} \qquad (2)$$

$$\begin{cases} P_s = q_s P_{s-1} + P_{s-2}, \\ Q_s = q_s Q_{s-1} + Q_{s-2};\ s = 2, 3, \ldots, n. \end{cases}$$

Chú ý. Qua định nghĩa của giản phân ta thấy tử số P_s phụ thuộc vào q_0 nên P_s có thể là số nguyên âm hoặc dương. Còn Q_s luôn luôn là số nguyên dương vì Q_s không phụ thuộc vào q_0 mà chỉ phụ thuộc vào các số nguyên dương $q_1, q_2, \ldots, q_s$ với các phép tính cộng và nhân. Hơn nữa cũng vì vậy ta có dãy $Q_0, Q_1, \ldots, Q_s$ là dãy các số nguyên dương tăng dần.

II – HỆ QUẢ. *Số hữu tỷ biểu thị bởi phân số δ_s bằng số hữu tỷ biểu thị bởi biểu thức*

$$q_0 + \cfrac{1}{q_1 + \cfrac{\ddots}{\ddots + \cfrac{1}{q_s}}},$$

cụ thể là ta có đẳng thức

$$\delta_s = q_0 + \cfrac{1}{q_1 + \cfrac{\ddots}{\ddots + \cfrac{1}{q_s}}}.$$

Chứng minh. Thật vậy, ta có

$$\delta_0 = \frac{P_0}{Q_0} = \frac{q_0}{1} = q_0;$$

$$\delta_1 = \frac{P_1}{Q_1} = \frac{q_1 q_0 + 1}{q_1} = q_0 + \frac{1}{q_1};$$

$$\delta_2 = \frac{P_2}{Q_2} = \frac{q_2 p_1 + p_o}{q_2 Q_1 + Q_o} = \frac{q_2(q_1 q_o + 1) + q_o}{q_2 q_1 + 1}$$

$$= q_o + \frac{q_2}{q_2 q_1 + 1} = q_o + \cfrac{1}{q_1 + \cfrac{1}{q_2}}$$

nghĩa là mệnh đề đã đúng với $s = 0, 1, 2$.

Giả sử mệnh đề đã đúng với $s = 0, 1, 2, \ldots, k$ $(k < n)$, ta phải chứng minh mệnh đề cũng đúng với $s = k + 1$.

Theo giả thiết qui nạp ta đã có

$$\delta_k = \frac{P_k}{Q_k} = \frac{q_k P_{k-1} + P_{k-2}}{q_k Q_{k-1} + Q_{k-2}} = q_o + \cfrac{1}{q_1 + \cfrac{\ddots}{\ddots + \cfrac{1}{q_k}}} \quad (3)$$

Ta hãy xét biểu thức

$$q_o + \cfrac{1}{q_1 + \cfrac{\ddots}{\ddots + \cfrac{1}{q_k + \cfrac{1}{q_{k+1}}}}} \quad (3')$$

Ta nhận thấy rằng các biểu thức (3) và (3') chỉ khác nhau ở số hạng cuối cùng, nghĩa là để tính giá trị của biểu thức (3') ta có thể thay vào biểu thức (3) ở chỗ q_k bởi $q_k + \frac{1}{q_{k+1}}$. Trong biểu thức (3) các số P_{k-1}, Q_{k-1}, P_{k-2}, Q_{k-2} không phụ thuộc vào q_k vì thế ta có

$$q_o + \cfrac{1}{q_1 + \cfrac{\ddots}{\ddots + \cfrac{1}{q_k + \cfrac{1}{q_{k+1}}}}} = \frac{\left(q_k + \frac{1}{q_{k+1}}\right) P_{k-1} + P_{k-2}}{\left(q_k + \frac{1}{q_{k+1}}\right) Q_{k-1} + Q_{k-2}}$$

$$= \frac{(q_k q_{k+1} + 1) P_{k-1} + q_{k+1} P_{k-2}}{(q_k q_{k+1} + 1) Q_{k-1} + q_{k+1} Q_{k-2}} =$$

$$= \frac{q_{k+1}(q_k P_{k-1} + P_{k-2}) + P_{k-1}}{q_{k+1}(q_k Q_{k-1} + Q_{k-2}) + Q_{k-1}} =$$

$$= \frac{q_{k+1} P_k + P_{k-1}}{q_{k+1} Q_k + Q_{k-1}} = \frac{P_{k+1}}{Q_{k+1}} = \delta_{k+1}.$$

Đến đây định lý được chứng minh hoàn toàn.

Chú ý rằng định lý này chứng tỏ rằng giá trị của một liên phân số hữu hạn cấp n bằng giá trị của giản phân cuối cùng δ_n của nó.

III – CÁCH THỰC HÀNH TÍNH CÁC GIẢN PHÂN. Trong thực hành, để tính các giản phân ta lập bảng như dưới đây rồi tính dần dần các giản phân từ giản phân thứ o trở đi.

s	o	1	2	...	k − 2	k − 1	k	...
q_s	q_o	q_1	q_2	...	q_{k-2}	q_{k-1}	q_k	...
P_s	q_o	$q_1 q_o + 1$	P_2	...	P_{k-2}	P_{k-1}	$q_k P_{k-1} + P_{k-2}$	...
Q_s	1	q_1	Q_2	...	Q_{k-2}	Q_{k-1}	$q_k Q_{k-1} + Q_{k-2}$	...

Ví dụ : Xét liên phân số $\frac{924}{330} = [2;\ 1, 1, 3, 4]$ ta có bảng các giản phân sau đây :

1	0	1	2	3	4
q_s	2	1	1	3	4
P_s	2	3	5	18	77
Q_s	1	1	2	7	30

IV — TÍNH CHẤT CÁC GIẢN PHÂN. Để cho gọn mà cũng không sợ lầm lẫn, ta dùng tiếng giản phân để biểu thị giá trị của nó.

1. Các giản phân đều là những phân số tối giản.

Chứng minh. Ta đặt

$$P_{s-1}Q_s - P_sQ_{s-1} = \Delta_s,\ 1 \leqslant s \leqslant n.$$

Theo công thức (2) ta có

$$P_{s-1}Q_s - P_sQ_{s-1} = P_{s-1}(q_sQ_{s-1} + Q_{s-2}) - (q_sP_{s-1} + P_{s-2})Q_{s-1} =$$
$$= -(P_{s-2}Q_{s-1} - P_{s-1}Q_{s-2})$$

nên

$$\Delta_s = -\Delta_{s-1}$$

Nhưng $\Delta_1 = P_0Q_1 - P_1Q_0 = q_1q_0 - (q_1q_0 + 1) = -1$ bởi vậy với mọi $s = 1, 2, \ldots, n$ ta có

$$\Delta_s = P_{s-1}Q_s - P_sQ_{s-1} = (-1)^s. \qquad (4)$$

Đẳng thức (4) cho ta điều cần chứng minh.

Từ tính chất này ta suy ra rằng nếu $\frac{a}{b}$ là phân số tối giản với $b > 0$ và $\frac{P_n}{Q_n}$ là giản phân cuối cùng của liên phân số biểu diễn nó thì $P_n = a$, $Q_n = b$.

2. Trong hai giản phân liên tiếp thì giản phân cấp lẻ lớn hơn giản phân cấp chẵn.

Chứng minh. Để chứng minh ta hãy xét hiệu

$$\delta_{s-1} - \delta_s.$$

Ta có

$$\delta_{s-1} - \delta_s = \frac{P_{s-1}}{Q_{s-1}} - \frac{P_s}{Q_s} = \frac{P_{s-1}Q_s - P_sQ_{s-1}}{Q_{s-1}Q_s} =$$
$$= \frac{\Delta_s}{Q_{s-1}Q_s} = \frac{(-1)^s}{Q_{s-1}Q_s}$$

Bởi vì Q_{s-1}, Q_s là những số nguyên dương nên $\frac{(-1)^s}{Q_{s-1}Q_s}$ là dương khi s là số chẵn, là âm khi s là số lẻ, do đó từ đẳng thức

$$\delta_{s-1} - \delta_s = \frac{(-1)^s}{Q_{s-1}Q_s} \tag{5}$$

ta suy ra điều cần chứng minh.

3. Tập hợp các giản phân cấp chẵn lập thành một dãy số hữu tỷ tăng cùng với chỉ số, còn tập hợp các giản phân cấp lẻ lập thành một dãy số hữu tỷ giảm khi chỉ số tăng.

Chứng minh. Với $s \geqslant 2$ ta có

$$\delta_{s-2} - \delta_s = \delta_{s-2} - \delta_{s-1} + \delta_{s-1} - \delta_s = \frac{(-1)^{s-1}}{Q_{s-2}Q_{s-1}} + \frac{(-1)^s}{Q_{s-1}Q_s} =$$

$$= (-1)^{s-1}\left(\frac{Q_s - Q_{s-2}}{Q_{s-2}Q_{s-1}Q_s}\right) = (-1)^{s-1}\left(\frac{q_sQ_{s-1} + Q_{s-2} - Q_{s-2}}{Q_{s-2}Q_{s-1}Q_s}\right),$$

tức là

$$\delta_{s-2} - \delta_s = \frac{(-1)^{s-1}q_s}{Q_{s-2}Q_s}. \tag{6}$$

Nhưng Q_{s-2}, Q_s là những số nguyên dương và với $s \geqslant 2$ có $q_s > 0$ cho nên từ đẳng thức (6) ta suy ra điều cần chứng minh.

4. Mỗi giản phân cấp chẵn nhỏ hơn mọi giản phân cấp lẻ.

Chứng minh. Ta hãy so sánh δ_{2s} và δ_{2r+1} với nhau.

Nếu $r = s$ thì theo tính chất 2 ta có $\delta_{2s} < \delta_{2r+1}$.

Nếu $r < s$ thì $2r + 1 < 2s + 1$ nên theo tính chất 3 có $\delta_{2s+1} < \delta_{2r+1}$ và theo tính chất 2 có $\delta_{2s} < \delta_{2s+1}$ do đó $\delta_{2s} < \delta_{2r+1}$.

Nếu $r > s$ thì $2r > 2s$ nên theo tính chất 3 có $\delta_{2r} > \delta_{2s}$ và theo tính chất 2 có $\delta_{2r} < \delta_{2r+1}$, do đó $\delta_{2s} < \delta_{2r+1}$.

Như vậy trong mọi trường hợp đều có $\delta_{2s} < \delta_{2r+1}$ nên ta suy ra điều cần chứng minh.

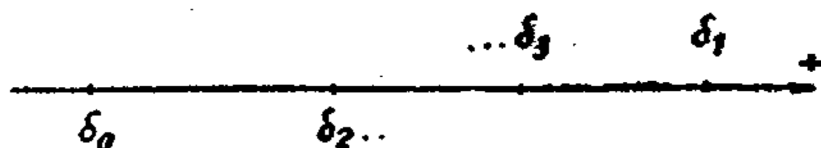
Chú ý. 1) Ta gọi *giá trị của liên phân số* (1) là giá trị của giản phân cuối cùng của nó. Như vậy, giá trị của

một liên phân số lớn hơn mọi giản phân cấp chẵn và bé hơn mọi giản phân cấp lẻ (dĩ nhiên không kể giản phân cuối cùng) của nó.

2) Từ các hệ thức (5) và (6) ta có

$$|\delta_s - \delta_{s-1}| \leqslant |\delta_s - \delta_{s-2}|, \quad s \geqslant 2, \tag{7}$$

nghĩa là trên trục số thì δ_s gần δ_{s-1} hơn là δ_{s-2}. Trong hệ thức (7) dấu bằng chỉ xảy ra trong trường hợp $s = 2$ với $q_1 = q_2 = 1$. Ta có hình ảnh hình học của dãy các giản phân trên trục số như sau:



§ 3. LIÊN PHÂN SỐ VÔ HẠN

1 — ĐỊNH NGHĨA. Cho α là một số vô tỉ. Bằng cách tách phần nguyên và phần phân của α ta có

$$\alpha = [\alpha] + \{\alpha\}.$$

Nhưng $0 < \{\alpha\} < 1$ nên ta đặt $\{\alpha\} = \frac{1}{\alpha_1}$ và $[\alpha] = q_0$ ta được

$$\alpha = q_0 + \frac{1}{\alpha_1}, \quad \alpha_1 > 1.$$

α_1 là một số vô tỉ vì nếu α_1 là hữu tỷ thì α sẽ là số hữu tỷ, bởi vậy lặp lại cách làm như trên đặt $\{\alpha_1\} = \frac{1}{\alpha_2}$ và $[\alpha_1] = q_1$ ta được

$$\alpha_1 = q_1 + \frac{1}{\alpha_2}$$

và

$$\alpha = q_0 + \cfrac{1}{q_1 + \cfrac{1}{\alpha_2}},$$

trong đó $q_1 \geqslant 1$ và α_2 là một số vô tỷ lớn hơn 1.

Cứ tiếp tục quá trình ấy, chẳng hạn s lần ta nhận được số vô tỷ $\alpha_{s-1} > 1$, bằng cách đặt $\{\alpha_{s-1}\} = \frac{1}{\alpha_s}$ và $[\alpha_{s-1}] = q_{s-1}$ ta được

$$\alpha_{s-1} = q_{s-1} + \frac{1}{\alpha_s}$$

và

$$\alpha = q_0 + \cfrac{1}{q_1 + \cfrac{\ddots}{+ \cfrac{1}{q_{s-1} + \cfrac{1}{\alpha_s}}}}. \tag{8}$$

Quá trình làm như trên kéo dài vô hạn (vì $\alpha_1, \alpha_1, \alpha_2, \ldots$ $\alpha_{s-1}, \alpha_s, \ldots$ đều là các số vô tỷ) và ta được một biểu thức dạng:

$$q_0 + \cfrac{1}{q_1 + \cfrac{1}{q_2 + \cfrac{\ddots}{+ \cfrac{1}{q_{s-1} + \cfrac{1}{q_s + \ddots}}}}} \tag{9}$$

Biểu thức (9) gọi là *một liên phân số vô hạn.*

Vậy *liên phân số vô hạn* là một biểu thức có dạng

$$q_0 + \cfrac{1}{q_1 + \cfrac{1}{q_2 + \cfrac{\ddots}{\ddots + \cfrac{1}{q_s + \ddots}}}} \qquad (9)$$



ký hiệu là

$$[q_0; q_1, \ldots, q_s, \ldots],$$

trong đó q_0 là một số nguyên tùy ý, $q_1, q_2, \ldots, q_s, \ldots$ là những số nguyên dương. Số nguyên q_s ($s = 0, 1, 2, \ldots$) được gọi là *số hạng thứ s* hay *thương hụt thứ s* của liên phân số (9).

II — GIẢN PHÂN

1. Định nghĩa. Ta gọi là *giản phân cấp s* (hay giản phân thứ s) với $s = 0, 1, 2, \ldots$ của liên phân số (9) là phân số $\delta_s = \dfrac{P_s}{Q_s}$, trong đó P_s và Q_s được xác định như sau

$$\begin{cases} P_0 = q_0, \\ Q_0 = 1; \end{cases} \qquad \begin{cases} P_1 = q_1 q_0 + 1, \\ Q_1 = q_1; \end{cases} \qquad (10)$$

$$\begin{cases} P_s = q_s P_{s-1} + P_{s-2}, \\ Q_s = q_s Q_{s-1} + Q_{s-2}, \quad s = 2, 3, \ldots \end{cases}$$

2. Hệ quả. Giản phân cấp s của một liên phân số vô hạn được định nghĩa hoàn toàn như giản phân cấp s của một liên phân số hữu hạn (I. § 2), bởi vậy ta cũng có kết quả như ở II. §2 là

$$\delta_s = q_0 + \cfrac{1}{q_1 + \cfrac{\ddots}{\ddots + \cfrac{1}{q_s}}}$$

Hơn nữa giản phân δ_s của một liên phân số vô hạn chỉ phụ thuộc vào $s+1$ thương hụt đầu tiên $q_0, q_1, \ldots, q_s$ nên các tính chất của giản phân đã nêu ở IV. § 2 vẫn đúng cả cho trường hợp liên phân số vô hạn.

3. Giá trị của một liên phân số vô hạn

Giả sử cho liên phân số vô hạn

$$[q_0 ; q_1, \ldots, q_s, \ldots]$$

và các giản phân $\delta_s = \frac{P_s}{Q_s} (s = 0, 1, \ldots)$ của nó. Ta thấy rằng khi s tăng lên vô hạn thì Q_s trở nên vô cùng lớn, vì thế từ biểu thức

$$\delta_{s-1} - \delta_s = \frac{(-1)^s}{Q_{s-1}Q_s}$$

ta có kết quả

$$\lim_{s \to \infty} (\delta_{s-1} - \delta_s) = 0$$

nghĩa là khoảng cách giữa hai giản phân liên tiếp của một liên phân số vô hạn giảm dần tới không khi chỉ số của các giản phân này tăng vô hạn. Hơn nữa những tính chất của giản phân còn chứng tỏ rằng dãy các giản phân cấp chẵn và dãy các giản phân cấp lẻ của mỗi liên phân số vô hạn đều hội tụ tới cùng một giá trị, vì vậy dãy các giản phân hội tụ, nói khác đi là có $\lim_{s \to \infty} \delta_s$ dĩ nhiên $\lim_{s \to \infty} \delta_s$ là một số vô tỷ và người ta gọi nó là giá trị của liên phân số đã cho.

Vậy ta gọi $\lim_{s \to \infty} \delta_s$ là *giá trị của liên phân số vô hạn*

$$[q_0 ; q_1, \ldots q_s, \ldots].$$

Đến đây để cho gọn, ta phát biểu định nghĩa giá trị của một liên phân số như sau:

Giá trị của một liên phân số hữu hạn là một số thực bằng giá trị giản phân cuối cùng của nó.

Giá trị của một liên phân số vô hạn là một số thực bằng giới hạn của các giản phân của nó.

III — BIỂU DIỄN MỘT SỐ THỰC THÀNH LIÊN PHÂN SỐ

Cho một số thực α, ta đặt $[\alpha]=q_0$. Nếu α không là số nguyên thì ắt có số thực $\alpha_1 > 1$ sao cho

$$\alpha = q_0 + \frac{1}{\alpha_1}$$

và ta lại đặt $[\alpha_1] = q_1$. Nếu α_1 không nguyên thì ắt có số thực $\alpha_2 > 1$ sao cho

$$\alpha_1 = q_1 + \frac{1}{\alpha_2}$$

và ta được

$$\alpha = q_0 + \cfrac{1}{q_1 + \cfrac{1}{\alpha_2}}, \quad \alpha_2 > 1.$$

Cứ tiếp tục quá trình tách phần nguyên như vậy chẳng hạn s lần (khi mà ta còn chưa gặp một số nguyên) ta được đẳng thức

$$\alpha = q_0 + \cfrac{1}{q_1 + \cfrac{1}{q_2 + \cdot \atop \cdot \; \cdot + \cfrac{1}{q_{s-1} + \cfrac{1}{\alpha_s}}}},$$

trong đó q_0 là một số nguyên, $q_1, q_2, \ldots, q_{s-1}$ là những số nguyên dương và $\alpha_s > 1$.

Nếu α là một *số hữu tỷ* thì quá trình trên đây là hữu hạn, nghĩa là ắt có α_n sao cho $q_n = [\alpha_n] = \alpha_n$. Thật vậy, giả sử $\alpha = \frac{a}{b}$, a, b là những số nguyên và $b > 0$. Khi

ấy quá trình tách phần nguyên trên dãy bắt đầu từ α chẳng qua là quá trình tìm các số thương hụt trong thuật toán Ơclid thực hiện trên hai số a, b, vì thế quá trình này phải kết thúc và ta có

$$\alpha = q_0 + \cfrac{1}{q_1 + \cfrac{1}{q_2 + \cdots + \cfrac{1}{q_n}}}.$$

trong đó q_0 là số nguyên, $q_1, q_2, ..., q_n$ là những số nguyên dương và $q_n > 1$. Vậy số thực α đã được biểu diễn bởi một liên phân số hữu hạn.

Nếu α là một *số vô tỷ* thì $\alpha_1, \alpha_2, ..., \alpha_s$ ... đều là vô tỷ cả, và do đó quá trình tách phần nguyên ở trên là vô hạn cho nên khi đó ta được một liên phân số vô hạn hoàn toàn xác định

$$q_0 + \cfrac{1}{q_1 + \cfrac{1}{q_2 + \cdots + \cfrac{1}{q_{s-1} + \cfrac{1}{q_s + \cdots}}}}.$$

Người ta chứng minh được rằng giá trị của liên phân số này chính bằng α, vậy ta có

$$\alpha = [q_0 ; q_1, q_2, ..., q_{s-1}, q_s, ...].$$

Ta đã chứng minh rằng mỗi số hữu tỷ $\alpha = \frac{a}{b}$ có một cách biểu diễn duy nhất thành liên phân số (2. III. § 1). Người ta cũng đã chứng minh được rằng mỗi số thực cho trước có duy nhất một cách biểu diễn thành liên phân số

Ví dụ. Biểu diễn $\alpha = \sqrt{2}$ thành liên phân số.

Ta có $q_0 = [\alpha] = 1$ và

$$\sqrt{2} = 1 + \frac{1}{\alpha_1}, \quad \alpha_1 = \frac{1}{\sqrt{2} - 1} = \sqrt{2} + 1$$

do đó có $q_1 = [\alpha_1] = 2$ và

$$\sqrt{2} + 1 = 2 + \frac{1}{\alpha_2}, \quad \alpha_2 = \frac{1}{\sqrt{2} - 1} = \alpha_1.$$

Từ $\alpha_1 = \alpha_1$ suy ra $q_s = q_1 = 2$, $s = 1, 2, \ldots$ và ta được:

$$\sqrt{2} = [1;\ 2\ \ 2,\ 2,\ \ldots].$$

Một liên phân số như vậy gọi là *liên phân số vô hạn tuần hoàn* với chu kỳ là (2) gồm một số và ta viết

$$\sqrt{2} = [1;\ 2,\ 2.\ 2,\ \ldots] = [1;\ (2)].$$

Nhưng không phải bao giờ ta cũng gặp may mắn như thế. Lagrăng đã chứng minh được định lý: những số vô tỷ bậc hai (nghiệm vô tỷ của đa thức bậc hai với hệ số hữu tỷ) và chỉ chúng mới biểu diễn được dưới dạng một liên phân số vô hạn tuần hoàn.

Người ta cũng còn chứng minh được rằng: liên phân số vô hạn của số vô tỷ $\sqrt{A}$ bao giờ cũng có dạng

$$\sqrt{A} = [q_0;\ (q_1, q_2, \ldots, q_2, q_1, 2q_0)]. \qquad (11)$$

Chẳng hạn

$$\sqrt{11} = [3;\ (3,\ 6)],$$
$$\sqrt{29} = [5;\ (2,\ 1,\ 1,\ 2,\ 10)].$$

Như vậy với những số vô tỷ không phải là đại số bậc hai nói chung ta chỉ biết được một số số hạng đầu tiên của liên phân số biểu diễn nó.

Chẳng hạn: :

$$\sqrt[3]{2} = [1;\ 3,\ 1,\ 5,\ 1,\ 1,\ \ldots];$$
$$\pi = [3;\ 7,\ 15,\ 1,\ 292,\ 1,\ \ldots];$$
$$e = [2;\ 1,\ 2,\ 1,\ 1,\ 4,\ 1,\ 1,\ 6\ \ldots]$$

nghĩa là: $q_0 = 2$, $q_1 = 1$, $q_{3s-1} = 2s$, $q_{3s} = q_{3s+1} = 1$, $s = 1, 2, \ldots$

Dựa vào công thức (10) của định nghĩa giản phân (1. II. § 3) ta tính được các giản phân đầu tiên của một liên phân số theo các thương hụt q_o, q_1, q_2, ... của nó.

Ví dụ: Với $\sqrt{2} = [1; (2)]$ ta có bảng các giản phân đầu tiên của nó là

s	0	1	2	3	4	5	6	...
q_s	1	2	2	2	2	2	2	...
P_s	1	3	7	17	41	99	239	...
Q_s	1	2	5	12	29	70	169	...

Với $\pi = [3, 7, 15, 1, 292, 1, ...]$ ta có bảng các giản phân đầu tiên của nó là

s	0	1	2	3	4	5	...
q_s	3	7	15	1	292	1	...
P_s	3	22	333	355	103 993	104 348	...
Q_s	1	7	106	113	33102	33215	...

Chú ý. Cho liên phân số

$$\alpha = [q_o; q_1, q_2, ..., q_k, q_{k+1}, ...],$$

ta sẽ gọi liên phân số

$$\alpha_k = [q_k; q_{k+1}, ...] \qquad (12)$$

là dư cấp k của liên phân số đã cho. Trong trường hợp liên phân số đã cho là hữu hạn cấp n thì đương nhiên phải có $k \leqslant n$. Như thông thường đẳng thức (12) còn biểu thị rằng giá trị của liên phân số dư $[q_k; q_{k+1}, ...]$ bằng số thực α_k và ta có $\alpha_k > 1$ với $k = 1, 2, ...$

Có thể chứng minh được rằng giữa α và α_k có sự liên hệ

$$\alpha = q_0 + \cfrac{1}{q_1 + \cfrac{1}{q_2 + \cdots + \cfrac{1}{q_{k-1} + \cfrac{1}{\alpha_k}}}},$$

nghĩa là để tính α ta thay q_k trong biểu thức tính giản phân cấp k là δ_k bởi α_k, cụ thể là ta có đẳng thức

$$\alpha = \frac{\alpha_k P_{k-1} + P_{k-2}}{\alpha_k Q_{k-1} + Q_{k-2}}. \qquad (13)$$

§4. ỨNG DỤNG CỦA LIÊN PHÂN SỐ

Trong tiết này chúng ta nêu lên vài ứng dụng đơn giản của liên phân số. Trong các bài sau chúng ta sẽ đưa thêm vài ứng dụng khác.

I. Như ở bài thứ nhất ta đã biết, điều kiện cần và đủ để cho hai số nguyên a và b nguyên tố cùng nhau là có hai số nguyên x_o và y_o sao cho $ax_o + by_o = 1$. Nhờ công cụ liên phân số ta có thể chỉ ra hai số nguyên x_o, y_o đó. Giả sử $(a, b) = 1$ và $b > 0$. Bằng cách biểu diễn $\frac{a}{b}$ thành liên phân số ta được

$$\frac{a}{b} = [q_o ; q_1, \dots, q_n]$$

và giả sử $\frac{P_{n-1}}{Q_{n-1}}$, $\frac{P_n}{Q_n}$ là hai giản phân cuối cùng của nó.

Khi ấy vì $b > 0$ và $(a, b) = 1$ phải có $P_n = a$, $Q_n = b$, và theo công thức (4) (IV, § 1) ta có

$$P_{n-1}Q_n - P_nQ_{n-1} = (-1)^n$$

hay

$$a(-1)^{n-1} Q_{n-1} + b(-1)^n P_{n-1} = 1. \quad (14)$$

Đẳng thức (14) chứng tỏ cặp số nguyên x_o, y_o cần tìm là

$$\begin{cases} x_o = (-1)^{n-1} Q_{n-1}, \\ y_o = (-1)^n P_{n-1}. \end{cases}$$

II – BIỂU DIỄN XẤP XỈ SỐ THỰC BẰNG CÁC GIẢN PHÂN

Cho α là một số thực và $[q_o; q_1, ..., q_s, ...]$ là liên phân số biểu diễn nó với các giản phân là

$$\delta_o = \frac{P_o}{Q_o}, \quad \delta_1 = \frac{P_1}{Q_1} \ ..., \delta_s = \frac{P_s}{Q_s} \ ....,$$

Người ta đã chứng minh được rằng nếu $\alpha \neq \delta_{s+1}$ thì có

$$\frac{1}{Q_s(Q_s + Q_{s+1})} < |\alpha - \delta_s| < \frac{1}{Q_s Q_{s+1}}. \quad (15)$$

Như vậy, nếu dùng giản phân để biểu diễn gần đúng số thực thì ta biết được cả cận trên và cận dưới của sai số. Người ta cũng chứng minh được rằng mỗi giản phân cấp s, $\frac{P_s}{Q_s}$ biểu diễn xấp xỉ số thực α một cách tốt nhất so với các phân số có mẫu số không vượt quá Q_s, nghĩa là nếu $0 < y \leqslant Q_s$ thì

$$\left|\alpha - \frac{P_s}{Q_s}\right| \leqslant \left|\alpha - \frac{x}{y}\right|$$

với mọi phân số $\frac{x}{y} \neq \alpha$.

Từ đó ta thấy rằng có thể dùng giản phân để biểu diễn xấp xỉ số thực với độ chính xác cao, bằng những số không lớn lắm. Tất cả những điều trên đây giải thích chẳng hạn như tại sao người ta đã dùng các phân số

$\frac{22}{7}$, $\frac{333}{106}$, $\frac{355}{113}$ để thay cho số π. Như ta đã biết đó chính là những giản phân của liên phân số biểu diễn số π.

Ta thấy:

$$\left|\pi - \frac{355}{113}\right| < \frac{1}{113.32102} < 0{,}0000003$$

nên nếu dùng giản phân $\frac{355}{113}$ biểu diễn số π ta mắc sai số nhỏ hơn một phần triệu. Trong khi đó muốn biểu diễn số π bằng phân số thập phân với sai số như vậy ta phải dùng số 3,1415926 hay phân số $\frac{15707963}{5000000}$.

Trong thực tế người ta dùng phân số $\frac{355}{113}$ mà không dùng phân số $\frac{333}{106}$ để biểu diễn số π vì các số 355 và 113 không lớn hơn các số 333 và 106 là mấy, mà $\frac{355}{113}$ lại cho số π với một độ chính xác vượt xa khi ta thay số π bằng $\frac{333}{106}$, vì giản phân tiếp theo $\frac{355}{113}$ có mẫu số là 33102 còn giản phân tiếp theo $\frac{333}{106}$ có mẫu số là 113.

BÀI TẬP

4.1. Biểu diễn các số hữu tỷ sau đây thành liên phân số

$$\frac{127}{52}\ ;\ -\frac{83}{217}\ ;\ 1,\ 23\ ;\ 0{,}00012.$$

4.2. Tìm dạng phân số của các liên phân số sau đây:

$[0; 1, 2, 3, 4, 5]$; $[1; 10, 100, 1000, 10000]$;

$[a; a, a, a, a]$; $[a; b, a, b, a]$.

4.3. Chứng minh rằng

a) $\left(\frac{P_{s+2}}{P_s} - 1\right)\left(1 - \frac{P_{s-1}}{P_{s+1}}\right) = \left(\frac{Q_{s+2}}{Q_s} - 1\right)\left(1 - \frac{Q_{s-1}}{Q_{s+1}}\right)$;

b) $P_{s+2}Q_{s-2} - P_{s-2}Q_{s+2} = (-1)^s(q_{s+2}q_{s+1}q_s + q_{s+2} + q_s)$;

c) $\frac{P_s}{Q_s} - \frac{P_0}{Q_0} = \frac{1}{Q_0Q_1} - \frac{1}{Q_1Q_2} + \dots + \frac{(-1)^{s+1}}{Q_{s-1}Q_s}$, trong đó

$\frac{P_s}{Q_s}$ $(s = 0, 1, \dots)$ là các giản phân của cùng một liên phân số

4.4. Cho liên phân số $[q_0; q_1, \dots, q_n]$ với $q_0 > 1$, $n > 1$. Chứng minh rằng

a) $\frac{P_n}{P_{n-1}} = [q_n; q_{n-1}, \dots, q_0]$; b) $\frac{Q_n}{Q_{n-1}} = [q_n; q_{n-1}, \dots, q_1]$.

4.5. Chứng minh các phân số $\frac{P_s}{P_{s-1}}$ và $\frac{Q_s}{Q_{s-1}}$ là tối giản.

4.6. Chứng minh rằng

$$[2; 2, \dots, 2] = \frac{(1+\sqrt{2})^{n+1} - (1-\sqrt{2})^{n+1}}{(1+\sqrt{2})^n - (1-\sqrt{2})^n},$$

trong đó liên phân số $[2; 2, \dots, 2]$ có n số hạng.

4.7. Giả sử $[q_0; q_1, \dots, q_n]$ là một liên phân số đối xứng, nghĩa là $q_n = q_0$, $q_{n-1} = q_1, \dots$ Chứng minh rằng

$$P_{n-1} = Q_n.$$

4.8. Tìm dạng liên phân số vô hạn của các số sau đây và tìm số hữu tỷ xấp xỉ tốt nhất của chúng với sai số tuyệt đối nhỏ hơn 0,001:

a) $\sqrt{3}$; b) $\sqrt{11}$; c) $\frac{2+\sqrt{5}}{3}$.

4.9. Với a là một số nguyên dương cho trước, hãy chứng minh rằng

a) $\sqrt{a^2+1} = [a; (2a)]$;

b) $\sqrt{a^2-1} = [a-1; (1, 2a-2)]$; $(a>1)$;

c) $\sqrt{a^2+2} = [a; (a, 2a)]$,

d) $\sqrt{a^2-2} = [a-1; (1, a-2, 1, 2a-2)]$, $(a > 2)$;

e) $\sqrt{a(a+1)} = [a; (2, 2a)]$;

g) $\sqrt{a(a+2)} = [a; (1, 2a)]$;

h) $\sqrt{a^4+2a} = [a^2; (a, 2a^2)]$.

4.10. Biểu diễn các liên phân số sau đây dưới dạng căn thức

a) $[2; 3, (2, 1)]$;

b) $[0; 1, 1, 1, 1, (2, 2, 2)]$;

c) $[a; (b, a)]$, a, b là những số nguyên dương.

4.11. Chứng minh rằng tích của hai số thực biểu diễn bởi hai liên phân số $[a; b, a, b, a, \ldots]$ và

$$[0; b, a, b, a, \ldots] \text{ bằng } \frac{a}{b}.$$

4.12. Chứng minh rằng với $s \geq 2$ ta có

$$Q_s \geq 2^{\frac{s-1}{2}}.$$

4.13. Cho α là một số thực và $\tau > 1$. Chứng minh rằng bao giờ cũng tìm được phân số $\frac{a}{b}$ sao cho

$$\left|\alpha - \frac{a}{b}\right| < \frac{1}{b\tau}, \quad 0 < b \leq \tau.$$

4.14. Hãy tìm các phân số gần đúng tốt nhất hai nghiệm số của phương trình sau đây với sai số tuyệt đối nhỏ hơn 0,0001

a) $2x^2 - 10x + 7 = 0$; b) $4x^2 + 20x + 23 = 0$.

4.15. Chứng minh rằng:

a) $\frac{1+\sqrt{5}}{2} = [1; (1)]$;

b) dãy các giản phân của [1 ; (1)] là $\frac{P_n}{Q_n} = \frac{u_{n+2}}{u_{n+1}}$, trong đó u_n ($n = 1, 2, \ldots$) là dãy số Phibônaxi.

c) $u_n = \frac{1}{\sqrt{5}}(a^n - b^n)$, trong đó a, b là hai nghiệm của phương trình $x^2 - x - 1 = 0$, với $a > b$.

BÀI THỨ NĂM

PHƯƠNG TRÌNH NGUYÊN

Trong bài này chúng ta nghiên cứu một số dạng phương trình nguyên (phương trình với hệ số nguyên) và các nghiệm nguyên của chúng. Trong những phương trình loại ấy, chúng ta quan tâm đến những phương trình có vô số nghiệm nguyên mà ta thường gọi là *phương trình vô định* hay là *phương trình Điôphăng.*

Chúng ta nhận thấy rằng phương trình nguyên một ẩn bậc n

$$a_0x^n + a_1x^{n-1} + \ldots + a_{n-1}x + a_n = 0 \quad (n \geqslant 1) \quad (1)$$

nếu có nghiệm nguyên là x_0 thì x_0 phải là ước của số hạng tự do a_n, bởi vì ta có đẳng thức

$$-x_0(a_0x_0^{n-1} + a_1x_0^{n-2} + \ldots + a_{n-1}) = a_n.$$

Như vậy số nghiệm nguyên của phương trình (1) là hữu hạn và để tìm tất cả các nghiệm nguyên của nó, ta chỉ cần thử trong các ước của số hạng tự do a_n xem những ước nào nghiệm đúng phương trình.

Ví dụ. Phương trình

$$x^6 + 2x^5 + x^3 + 2 = 0$$

có nghiệm nguyên duy nhất là $x = -1$ bởi vì trong các ước 1, -1, 2 và -2 của số hạng tự do chỉ có -1 nghiệm

đúng phương trình này. Cũng bằng phương pháp như vậy dễ dàng thấy rằng phương trình

$$x^5 - x^2 + x - 5 = 0$$

không có nghiệm nguyên.

Bây giờ chúng ta nghiên cứu một số dạng phương trình vô định, dĩ nhiên như nhận xét ở trên, đó là những phương trình nhiều ẩn.

§ 1. PHƯƠNG TRÌNH BẬC NHẤT NHIỀU ẨN

I – PHƯƠNG TRÌNH BẬC NHẤT HAI ẨN

Xét phương trình

$$ax + by = c, \qquad (1)$$

trong đó a, b, c là những số nguyên cho trước và a, b đồng thời khác không.

Vấn đề đặt ra là với điều kiện ràng buộc nào giữa a, b và c thì phương trình (1) có nghiệm nguyên và khi có nghiệm nguyên thì việc xác định nghiệm của nó như thế nào?

1. Điều kiện có nghiệm nguyên.

a) Định lý. *Điều kiện cần và đủ để phương trình* (1) *có nghiệm nguyên là ước chung lớn nhất của các hệ số của các ẩn là ước của số hạng tự do.*

Chứng minh. Điều kiện cần. Giả sử phương trình (1) có nghiệm nguyên, nghĩa là có cặp số nguyên x_0, y_0 sao cho ta có đẳng thức $ax_0 + by_0 = c$. Gọi $d = (a, b)$, vì d chia hết a và b nên d chia hết $c = ax_0 + by_0$.

– *Điều kiện đủ.* Giả sử $d = (a, b)$ chia hết c, nghĩa là có số nguyên c_1 sao cho $c = dc_1$. Ta phải chứng minh rằng phương trình (1) có nghiệm nguyên, tức là có cặp số nguyên x_0, y_0 sao cho ta có đẳng thức

$ax_0 + by_0 = c$. Bởi vì $d = (a, b)$ nên ắt có cặp số nguyên x_1, y_1 sao cho $ax_1 + by_1 = d$. Nhân hai vế của đẳng thức này với c_1 ta được

$$a(c_1x_1) + b(c_1y_1) = c.$$

Điều này chứng tỏ cặp số nguyên $x_0 = c_1x_1$, $y_0 = c_1y_1$ là một nghiệm nguyên của phương trình (1).

b) **Hệ quả.** Nếu $(a, b) = 1$ thì phương trình (1) có nghiệm nguyên.

Về phương diện hình học, định lý trên cho ta điều kiện ràng buộc giữa a, b và c để đường thẳng $ax + by = c$ đi qua điểm có tọa độ nguyên (tung độ và hoành độ là những số nguyên). Vấn đề tiếp theo đặt ra là giả sử đường thẳng $ax + by = c$ (a, b, c là những số nguyên và $ab \neq 0$) đi qua một điểm nguyên $M(x_0, y_0)$ thì hỏi rằng nó còn đi qua điểm nguyên nào khác nữa không và nếu có thì tọa độ các điểm nguyên đó có liên hệ như thế nào với tọa độ x_0, y_0 của điểm M. Về phương diện đại số, giải quyết vấn đề này ta có kết quả sau đây.

2. Tập hợp nghiệm nguyên của phương trình (1)

Định lý : *Nếu phương trình* (1) *có một nghiệm nguyên x_0, y_0 thì nó có vô số nghiệm nguyên, đó là tập hợp tất cả các cặp số nguyên x, y có dạng*

$$\begin{cases} x = x_0 + \dfrac{b}{d}t, \\ y = y_0 - \dfrac{a}{d}t, \end{cases}$$

với $d = (a, b)$ và $t = 0, \pm 1, \pm 2 \ldots$

Chứng minh. Mọi cặp số nguyên $x_0 + \dfrac{b}{d}t$, $y_0 - \dfrac{a}{d}t$ đều là nghiệm của phương trình (1). Thật vậy, theo giả thiết x_0, y_0 là nghiệm của phương trình (1) nên ta có đẳng thức $ax_0 + by_0 = c$, từ đó

$$a\left(x_o + \frac{b}{d}t\right) + b\left(y_o - \frac{a}{d}t\right) = c.$$

Đẳng thức này chứng tỏ $x_o + \frac{b}{d}t$, $y_o - \frac{a}{d}t$ là một nghiệm nguyên của phương trình (1).

– Bây giờ giả sử x_1, y_1 là một nghiệm nguyên tùy ý của phương trình (1), ta phải chứng minh rằng ắt có số nguyên t sao cho

$$x_1 = x_o + \frac{b}{d}t,\ y_1 = y_o - \frac{a}{d}t.$$

Thật vậy, vì x_o, y_o và x_1, y_1 là hai nghiệm của phương trình (1) nên ta có

$$ax_o + by_o = c,$$
$$ax_1 + by_1 = c.$$

Các đẳng thức này cho ta

$$a(x_1 - x_o) = b(y_o - y_1)$$

hay là

$$\frac{a}{d}(x_1 - x_o) = \frac{b}{d}(y_o - y_1).$$

Đẳng thức sau cùng chứng tỏ $\frac{b}{d} \Big| \frac{a}{d}(x_1 - x_o)$. Nhưng $d = (a, b)$, tức là $\left(\frac{a}{d}, \frac{b}{d}\right) = 1$ nên $\frac{b}{d} \Big| x_1 - x_o$, nghĩa là có số nguyên t sao cho $x_1 - x_o = \frac{b}{d}t$ hay $x_1 = x_o + \frac{b}{d}t$. Từ đây cùng với đẳng thức $\frac{a}{d}(x_1 - x_o) = \frac{b}{d}(y_o - y_1)$ ta được $y_1 = y_o - \frac{a}{d}t$. Đến đây định lý được chứng minh.

Ví dụ. (Một bài toán cổ)

« Trăm trâu, trăm cỏ,
Trâu đứng ăn năm,
Trâu nằm ăn ba,
Lụ khụ trâu già
Ba con một bó ».

Hỏi có bao nhiêu trâu đứng, bao nhiêu trâu nằm và bao nhiêu trâu già?.

Gọi số trâu đứng là x, số trâu nằm là y thì số trâu già là $100 - (x+y)$ và ta có phương trình

$$5x + 3y + \frac{100 - (x + y)}{3} = 100.$$

Phương trình trên tương đương với phương trình

$$7x + 4y = 100.$$

Ta phải tìm nghiệm nguyên dương của phương trình này. Dễ thấy $x_0 = 0$, $y_0 = 25$ là một nghiệm nguyên của phương trình $7x + 4y = 100$ nên tập hợp nghiệm nguyên của nó gồm tất cả các cặp số nguyên x, y sau đây:

$$\begin{cases} x = 4t, \\ y = 25 - 7t \text{ với } t \text{ là số nguyên tùy ý.} \end{cases}$$

Bởi vì $x = 4t > 0$ và $y = 25 - 7t > 0$ nên ta phải có $0 < t < 4$, do đó số trâu đứng là $x = 4t$, số trâu nằm là $y = 25 - 7t$ và số trâu già là $75 + 3t$ với $t = 1, 2, 3$.

Tóm lại số trâu mỗi loại như sau

t	Số trâu đứng	Số trâu nằm	Số trâu già
1	4	18	78
2	8	11	81
3	12	4	84

Các kết quả trên đây cho ta thấy rằng muốn giải phương trình (1) trong điều kiện giải được, ta chỉ cần tìm một

nghiệm cụ thể nào đó của nó. Sau đây chúng ta nêu lên một cách xác định một nghiệm cụ thể của phương trình (1) bằng công cụ liên phân số.

3. Xác định một nghiệm nguyên của phương trình (1).

Để cho thuận tiện ta giả thiết $(a, b) = 1$ và $b > a$. Như đã tiến hành ở I §1 bài thứ tư, ta phân tích $\frac{a}{b}$ thành liên phân số $\frac{a}{b} = [q_0 ; q_1, ..., q_n]$ và giả sử $\frac{P_{n-1}}{Q_{n-1}}$ và $\frac{P_n}{Q_n}$ là hai giản phân cuối cùng của nó, khi ấy $P_n = a, Q_n = b$ và

$$P_{n-1} b - aQ_{n-1} = (-1)^n$$

hay là

$$a(-1)^{n-1}Q_{n-1} + b(-1)^n P_{n-1} = 1.$$

Đẳng thức này sau khi nhân hai vế với c cho

$$a[(-1)^{n-1} cQ_{n-1}] + b[(-1)^n cP_{n-1}] = c,$$

nghĩa là phương trình (1) có một nghiệm nguyên là

$$\begin{cases} x_0 = (-1)^{n-1} cQ_{n-1}, \\ y_0 = (-1)^n cP_{n-1}. \end{cases}$$

Ví dụ. Giải phương trình vô định

$$342x - 123y = 15.$$

Ta thấy $(342, 123) = 3$ là ước của 15 nên phương trình đã cho có nghiệm nguyên. Phương trình đã cho tương đương với phương trình

$$114x - 41y = 5.$$

Khai triển $\frac{114}{41}$ thành liên phân số ta được

$$\frac{114}{41} = [2; 1, 3, 1, 1, 4]$$

và hai giản phân cuối cùng của nó là

$$\frac{P_5}{Q_5} = \frac{114}{41}, \frac{P_4}{Q_4} = \frac{25}{9}.$$

Theo công thức tìm nghiệm,

$$\begin{cases} x_1 = 5.9 = 45, \\ y_1 = -5.25 = -125 \end{cases}$$

là một nghiệm nguyên của phương trình $114x + 41y = 5$, do đó phương trình $114x - 41y = 5$ có một nghiệm nguyên là

$$\begin{cases} x_0 = 45, \\ y_0 = 125 \end{cases}$$

và nghiệm tổng quát là

$$\begin{cases} x = 45 + 41t, \\ y = 125 + 114t \end{cases}$$

$$t = 0, \pm 1, \pm 2, \ldots$$

Đây cũng là nghiệm tổng quát của phương trình đã cho.

II – PHƯƠNG TRÌNH BẬC NHẤT NHIỀU ẨN

Chúng ta xét phương trình bậc nhất n ẩn

$$a_1x_1 + a_2x_2 + \ldots + a_nx_n = b, \qquad (2)$$

trong đó $a_1, a_2, \ldots, a_n$ và b là những số nguyên cho trước, $a_1, a_2, \ldots, a_n$ đồng thời khác không, còn n là một số tự nhiên lớn hơn 2.

1. Điều kiện có nghiệm nguyên.

a. Định lý. *Điều kiện cần và đủ để phương trình (2) có nghiệm nguyên là ước chung lớn nhất của các hệ số $a_1, a_2, \ldots, a_n$ của các ẩn là ước của số hạng tự do b.*

Việc chứng minh định lý này hoàn toàn tương tự như trường hợp n = 2 mà ta đã xét ở trên. Từ định lý này ta suy ra hệ quả sau đây:

b. Hệ quả. *Nếu $(a_1, a_2, \ldots, a_n) = 1$ thì phương trình (2) có nghiệm nguyên.*

Chúng ta không đi sâu nghiên cứu tập hợp nghiệm nguyên của phương trình (2) cũng như việc tìm biểu

thức cho nghiệm nguyên tổng quát của nó. Tuy nhiên có thể khẳng định rằng *trong trường hợp phương trình (2) có nghiệm nguyên thì nó có vô số nghiệm nguyên phụ thuộc vào n — 1 tham số.* Thật vậy giả sử $\alpha_1, \alpha_2, \ldots, \alpha_n$ là một nghiệm nguyên của phương trình (2) thì bằng cách thử ta sẽ thấy rằng tất cả các bộ n số nguyên $x_1, x_2, \ldots, x_n$ xác định như sau cũng nghiệm đúng phương trình (2)

$$\begin{cases} x_1 = \alpha_1 + a_n t_1, \\ x_2 = \alpha_2 + a_n t_2, \\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot \\ x_{n-1} = \alpha_{n-1} + a_n t_{n-1}, \\ x_n = \alpha_n - a_1 t_1 - a_2 t_2 - \ldots - a_{n-1} t_{n-1}, \end{cases}$$

trong đó $t_1, t_2, \ldots, t_{n-1}$ lấy tất cả các giá trị nguyên một cách độc lập với nhau.

2. Cách thực hành giải phương trình (2). Để đi đến một cách thực hành giải phương trình (2) ta nêu lên một số nhận xét sau đây:

a) Trước hết ta có thể giả thiết rằng các hệ số a_1 $a_2, \ldots, a_n$ của các ẩn trong phương trình (2) là nguyên tố cùng nhau và hơn nữa tất cả chúng đều là những số nguyên dương.

Thật vậy nếu $(a_1, a_2, \ldots, a_n) = d$ và $d \mid b$ thì sau khi chia cả hai vế của phương trình (2) cho d ta được một phương trình với hệ số của các ẩn là những số nguyên nguyên tố cùng nhau, tương đương với phương trình (2). Hơn nữa không làm mất tính tổng quát, giả sử a_1 là số nguyên âm thì ta đặt $a'_1 = -a_1$ là số nguyên dương.

Khi ấy nếu $\alpha_1, \alpha_2, \ldots, \alpha_n$ là một nghiệm nguyên của phương trình:

$$a'_1 x_1 + a_2 x_2 + \ldots + a_n x_n = b \qquad (2.a)$$

thì $-\alpha_1, \alpha_2, \ldots, \alpha_n$ là một nghiệm nguyên của phương trình (2). Ngược lại mỗi nghiệm nguyên $\beta_1, \beta_2, \ldots, \beta_n$ của phương trình (2) cho ta một nghiệm nguyên của phương trình (2.a) là $-\beta_1, \beta_2, \ldots, \beta_n$.

b) Nếu trong phương trình (2) có một hệ số nào đó bằng 1 thì việc tìm tất cả các nghiệm nguyên của nó cơ bản được giải quyết.

Thật vậy nếu chẳng hạn $a_1 = 1$ thì phương trình (2) có nghiệm nguyên là tất cả các bộ n số nguyên $x_1, x_2, \ldots, x_n$ xác định như sau :

$$\begin{cases} x_1 = -a_2t_2 - a_3t_3 - \ldots - a_nt_n + b, \\ x_2 = t_2, \\ \cdots\cdots \\ x_n = t_n, \end{cases}$$

trong đó $t_2, t_3, \ldots, t_n$ là những số nguyên tùy ý.

c) Nếu trong n hệ số $a_1, a_2, \ldots, a_n$ của các ẩn số có k hệ số bằng nhau ($2 \leqslant k \leqslant n$) thì việc tìm nghiệm nguyên của phương trình (2) được đưa về việc tìm nghiệm nguyên của một phương trình bậc nhất có $n-k+1$ ẩn.

Thật vậy, không làm mất tính tổng quát, giả sử $a_1 = a_2 = \ldots = a_k$. Khi ấy từ mỗi nghiệm nguyên $x_1 = \alpha_1$, $x_2 = \alpha_2, \ldots, x_n = \alpha_n$ của phương trình (2) ta được một nghiệm nguyên $x = \alpha_1 + \alpha_2 + \ldots + \alpha_k$, $x_{k+1} = \alpha_{k+1}, \ldots$ $x_n = \alpha_n$ của phương trình

$$a_1x + a_{k+1}x_{k+1} + \ldots + a_nx_n = b. \qquad (2.b)$$

Ngược lại từ mỗi nghiệm nguyên $x = \beta$, $x_{k+1} = \beta_{k+1}, \ldots$ $x_n = \beta_n$ của phương trình (2b), bằng cách lấy $x_1 = \beta_1$, $x_2 = \beta_2, \ldots, x_{k-1} = \beta_{k-1}$ là những số nguyên tùy ý và đặt $x_k = \beta - \beta_1 - \beta_2 - \ldots - \beta_{k-1}$, $x_{k+1} = \beta_{k+1}, \ldots, x_n = \beta_n$ ta được $x_1, x_2, \ldots, x_n$ là một nghiệm nguyên của phương trình (2).

d. Từ những nhận xét trên *ta có thể giả thiết rằng các hệ số $a_1, a_2, \ldots, a_n$ của các ẩn trong phương trình (2) là*

những số nguyên dương đôi một khác nhau và giả sử rằng $a_1 > a_2 > ... > a_n$.

Chia a_1 cho a_2 giả sử ta được

$$a_1 = a_2q + a'_2 , \ 0 < a'_2 < a_2.$$

Khi ấy bằng cách đặt ẩn phụ $x'_2 = qx_1 + x_2$ ta có phương trình

$$a_2x'_2 + a'_2x_1 + a_3x_3 + ... + a_nx_n = b. \qquad (2.c)$$

Ta thấy rằng từ mỗi nghiệm nguyên $x_1 = \alpha_1$, $x_2 = \alpha_2$,... $x_n = \alpha_n$ của phương trình (2) ta được một nghiệm nguyên của phương trình (2.c) là $x'_2 = q\alpha_1 + \alpha_2$, $x_1 = \alpha_1$, $x_3 = \alpha_3, ..., x_n = \alpha_n$. Ngược lại từ mỗi nghiệm nguyên $x'_2 = \beta_2$, $x_1 = \beta_1$, $x_3 = \beta_3, ..., x_n = \beta_n$ của phương trình (2.c) ta được một nghiệm nguyên của phương trình (2) là $x_1 = \beta_1$, $x_2 = \beta_2 - q\beta_1$, $x_3 = \beta_3, ..., x_n = \beta_n$.

Như vậy, để tìm nghiệm nguyên của phương trình (2) ta đưa về tìm nghiệm nguyên của phương trình (2.c) mà hệ số lớn nhất của ẩn ở phương trình (2.c) nhỏ hơn hệ số lớn nhất của ẩn ở phương trình (2). Nhưng $a_1, a_2, ..., a_n$ là những số nguyên dương cho nên sau một số hữu hạn bước làm như vậy ta sẽ đưa phương trình (2) về một phương trình bậc nhất với các hệ số của các ẩn là những số nguyên dương và có một trong các hệ số đó bằng 1 và việc tìm tất cả các nghiệm nguyên của phương trình (2) cơ bản được giải quyết.

Ví dụ. Giải phương trình vô định

$$6x + 45y + 6z - 10t = 13.$$

Phương trình đã cho được viết dưới dạng

$$6(x + z) + 45y - 10t = 13.$$

Bằng cách đặt $x+z = x', -t = t'$ ta được phương trình

$$6x'+45y+10t' = 13.$$

Vì $45 = 10 . 4+5$ nên phương trình này có thể viết dưới dạng

$$6x'+10(4y+t')+5y = 13$$

và bằng cách đặt $4y+t' = u$ ta được phương trình

$$6x' + 10u + 5y = 13.$$

Nhưng ở đây $6 = 5 . 1+1$, bởi vậy ta viết phương trình đó dưới dạng

$$5(x'+y)+x'+10u = 13.$$

và đặt $x'+y = v$ ta được phương trình

$$5v+x'+10u = 13.$$

Từ phương trình sau cùng này ta suy ra

$$x' = 13-10u-5v.$$

Thay giá trị của x' vào biểu thức $y = v-x'$ ta được

$$y = 6v + 10u - 13.$$

Thay giá trị của y vào biểu thức $t' = u-4y$ ta được

$$t' = 52 - 39u - 24v$$

cho nên $\quad t = -t' = -52 + 39u + 24v.$

Từ $x + z = x'$ ta có

$$x = x' - z = 13 - 10u - 5v - z.$$

Vậy phương trình đã cho có nghiệm nguyên là

$$\begin{cases} x = 13 - 10u - 5v - w, \\ y = -13 + 10u + 6v, \\ z = w, \\ t = -52 + 39u + 24v. \end{cases}$$

trong đó u, v, w là những số nguyên tùy ý.

e. Chú ý. *Nếu phương trình (2) có hai hệ số nào đó nguyên tố cùng nhau thì phương trình (2) có nghiệm nguyên và việc tìm nghiệm nguyên của phương trình (2) được đưa về việc tìm nghiệm nguyên của một phương trình bậc nhất hai ẩn.*

Thật vậy, không làm mất tính tổng quát giả sử $(a_1, a_2) = 1$. Khi ấy lấy $x_3 = \alpha_3$, $x_4 = \alpha_4, \ldots, x_n = \alpha_n$ là những số nguyên tùy ý thì phương trình

$$a_1 x_1 + a_2 x_2 = b - a_3 \alpha_3 - a_4 \alpha_4 - \ldots - a_n \alpha_n$$

có nghiệm nguyên $x_1 = \alpha_1$, $x_2 = \alpha_2$, ta được $x_1 = \alpha_1$, $x_2 = \alpha_2$, $x_3 = \alpha_3, \ldots, x_n = \alpha_n$ là một nghiệm nguyên của phương trình (2). Ngược lại nếu $x_1 = \beta_1$, $x_2 = \beta_2$, $x_3 = \beta_3, \ldots, x_n = \beta_n$ là nghiệm nguyên của phương trình (2) thì ta có đẳng thức

$$a_1 \beta_1 + a_2 \beta_2 = b - a_3 \beta_3 - \ldots - a_n \beta_n.$$

Ví dụ. Giải phương trình vô định

$$2x - 5y - 4z + 6t = 4.$$

Phương trình đã cho tương đương với phương trình

$$2x - 5y = 4 + 4z - 6t.$$

Lấy $z = u$, $t = v$ là những số nguyên tùy ý, đặt $4 + 4u - 6v = c$ ta được phương trình $2x - 5y = c$, có nghiệm nguyên là

$$\begin{cases} x = 3c + 5w, \\ y = c + 2w, \end{cases}$$

với w là số nguyên tùy ý. Vậy phương trình đã cho có nghiệm nguyên là :

$$\begin{cases} x = 12 + 12u - 18v + 5w, \\ y = 4 + 4u - 6v + 2w, \\ z = u, \\ t = v, \end{cases}$$

trong đó u, v, w là những số nguyên tùy ý.

III – HỆ PHƯƠNG TRÌNH BẬC NHẤT VỚI SỐ ẨN NHIỀU HƠN SỐ PHƯƠNG TRÌNH.

Chúng ta không có tham vọng nêu lên lý thuyết tổng quát về sự tồn tại nghiệm nguyên và cách tìm các nghiệm nguyên của hệ gồm m phương trình bậc nhất

n ẩn ($m < n$) với hệ số nguyên. Tùy nhiên có thể thấy rằng, nếu hệ phương trình đã cho không có phương trình nào là hệ quả của các phương trình còn lại của hệ thì khi hệ có nghiệm nguyên nó sẽ có vô số nghiệm nguyên phụ thuộc vào $n - m$ tham số.

Ví dụ. Tìm các nghiệm nguyên của hệ phương trình

$$\begin{cases} 4x - 5y + 5z = 7, \\ 5x - 7y + 10z = 13 \end{cases}$$

Hệ phương trình đã cho tương đương với hệ phương trình.

$$\begin{cases} 8x - 10y + 10z = 14, \\ 5x - 7y + 10z = 13. \end{cases}$$

Trừ vế với vế hai phương trình trên ta được

$$2x - 3y = 1.$$

Phương trình này có nghiệm nguyên tổng quát là

$$\begin{cases} x = 2 + 3t, \\ y = 1 + 2t, \end{cases}$$

với t là một số nguyên tùy ý.

Thay các biểu thức của x và y vào phương trình thứ nhất của hệ phương trình đã cho ta được

$$4(2 + 3t) - 5(1 + 2t) + 5z = 7, \text{ hay là } 2t + 5z = 4.$$

Phương trình này có nghiệm nguyên tổng quát là

$$\begin{cases} t = -3 + 5u, \\ z = 2 - 2u \end{cases}$$

với u là một số nguyên tùy ý.

Từ đó ta được tất cả các nghiệm nguyên của hệ phương trình đã cho là

$$\begin{cases} x = -7 + 15u, \\ y = -5 + 10u, \\ z = 2 - 2u, \end{cases}$$

trong đó u là một số nguyên tùy ý.

Bây giờ chúng ta xét một hệ gồm $n - 1$ phương trình bậc nhất n ẩn ($n > 2$) dạng

$$a_1x_1 + b_1 = a_2x_2 + b_2 = \ldots = a_nx_n + b_n, \qquad (3)$$

trong đó $a_1, a_2, \ldots, a_n$ và $b_1, b_2, \ldots, b_n$ là những số nguyên cho trước, $a_1, a_2, \ldots, a_n$ đồng thời khác 0 và nguyên tố cùng nhau từng đôi một.

1. Định lý Trung Hoa về thặng dư. *Với điều kiện $a_1, a_2, \ldots, a_n$ nguyên tố cùng nhau từng đôi một, hệ phương trình (3) có nghiệm nguyên.*

Chứng minh. Chúng ta chứng minh bằng phép qui nạp toán học theo n.

Định lý đúng với $n = 2$ bởi vì với $(a_1, a_2) = 1$ thì phương trình $a_1x_1 - a_2x_2 = b_2 - b_1$ có nghiệm nguyên.

Giả sử định lý đúng với số tự nhiên $n \geqslant 2$ ta sẽ chứng minh định lý đúng với số tự nhiên $n + 1$.

Thật vậy, giả sử $a_1, a_2, \ldots, a_n, a_{n+1}$ là những số nguyên khác không, đôi một nguyên tố cùng nhau và $b_1, b_2, \ldots, b_n, b_{n+1}$ là những số nguyên tùy ý. Từ giả thiết định lý đúng với n, ta có các số nguyên $x_1^o, x_2^o, \ldots, x_n^o$ sao cho xảy ra các đẳng thức

$$a_1x_1^o + b_1 = a_2x_2^o + b_2 = \ldots = a_nx_n^o + b_n.$$

Đặt $y_o = a_1x_1^o + b_1 = a_2x_2^o + b_2 = \ldots = a_nx_n^o + b_n$. Vì $a_1, a_2, \ldots, a_n, a_{n+1}$ nguyên tố cùng nhau từng đôi một, nên tích $a_1a_2 \ldots a_n$ nguyên tố với a_{n+1}, và phương trình

$$a_1a_2 \ldots a_nt - a_{n+1}u = b_{n+1} - y_o$$

có nghiệm nguyên, tức là có cặp số nguyên t_o, u_o sao cho

$$a_1a_2 \ldots a_nt_o - a_{n+1}u_o = b_{n+1} - y_o,$$

Khi ấy ta đặt

$$x_i^1 = \frac{a_1a_2 \ldots a_n}{a_i}t_o + x_i^o, \quad i = 1, 2, \ldots, n,$$

$$x_{n+1}^1 = u_o$$

thì $x_1^1, x_2^1, \ldots, x_n^1, x_{n+1}^1$ là một nghiệm nguyên của phương trình

$a_1x_1+b_1=a_2x_2+b_2= \ldots =a_nx_n+b_n=a_{n+1}x_{n+1}+b_{n+1}$ bởi vì với $i=1, 2, \ldots, n+1$ ta đều có

$$a_i x_i^1+b_i=a_1a_2\ldots a_nt_o+y_o.$$

Đến đây định lý được chứng minh hoàn toàn.

2. Tập hợp nghiệm nguyên của hệ phương trình (3).

Định lý. *Nếu hệ phương trình (3) có một nghiệm nguyên là $x_1^o, x_2^o, \ldots, x_n^o$, thì nó có vô số nghiệm nguyên và tập hợp nghiệm nguyên của nó gồm tất cả các bộ n số nguyên $x_1, x_2, \ldots, x_n$ có dạng*

$$x_i=x_i^o+\frac{a_1a_2\ldots a_n}{a_i}t, \; i = 1, 2, \ldots, n$$

với t là một số nguyên tùy ý.

Chứng minh. a). Đặt $a = a_1a_2\ldots a_n$, ta phải chứng minh rằng với số nguyên t tùy ý cho trước thì bộ n số nguyên $x_1^o+\frac{a}{a_1}t, x_2^o+\frac{a}{a_2}t, \ldots, x_n^o+\frac{a}{a_n}t$ là một nghiệm của hệ phương trình (3).

Thật vậy, theo giả thiết $x_1^o, x_2^o, \ldots, x_n^o$ là một nghiệm nguyên của hệ phương trình (3) nên ta có

$$a_1 x_1^o+b_1 = a_2x_2^o+b_2 = \ldots = a_nx_n^o+b_n=y_o.$$

Khi ấy rõ ràng với mọi $i=1, 2, \ldots, n$ ta có

$$a_i\left(x_i^o+\frac{a}{a_i}t\right)+b_i=a_ix_i^o+b_i+at=y_o+at$$

cho nên

$$a_1\left(x_1^o+\frac{a}{a_1}t\right)+b_1=a_2\left(x_2^o+\frac{a}{a_2}t\right)+b_2=\ldots=$$
$$=a_n\left(x_n^o+\frac{a}{a_n}t\right)+b_n.$$

Các đẳng thức sau cùng ở trên chứng tỏ rằng $x_1^o + \frac{a}{a_1}t$, $x_2^o + \frac{a}{a_2}t$, ..., $x_n^o + \frac{a}{a_n}t$ là một nghiệm nguyên của hệ phương trình (3).

b) Bây giờ giả sử $x_1^1, x_2^1, ..., x_n^1$ là một nghiệm nguyên tùy ý của hệ phương trình (3), ta phải chứng minh sự tồn tại của số nguyên t sao cho :

$$x_i^1 = x_i^o + \frac{a}{a_i}t,\ i = 1, 2, ..., n,$$

trong đó $a = a_1 a_2 ... a_n$.

Thật vậy vì theo giả thiết $x_1^o, x_2^o, ..., x_n^o$ và $x_1^1, x_2^1, ..., x_n^1$ là hai nghiệm nguyên của hệ phương trình (3) ta có

$$a_1 x_1^o + b_1 = a_2 x_2^o + b_2 = ... = a_n x_n^o + b_n = y_o$$

và

$$a x_1^1 + b_1 = a_2 x_2^1 + b_2 = ... = a_n x_n^1 + b_n = y_1.$$

Từ đó với i = 1,2 ,..., n ta được

$$a_i\left(x_i^1 - x_i^o\right) = y_1 - y_o.$$

Các đẳng thức này chứng tỏ $a_i \mid y_1 - y_o$, $i = 1, 2, ..., n$, nhưng $a_1, a_2, ..., a_n$ nguyên tố cùng nhau từng đôi một và $a = a_1 a_2 ... a_n$ nên ta suy ra

$$a \mid y_1 - y_o,$$

nghĩa là tồn tại số nguyên t sao cho

$$y_1 - y_o = at.$$

Sau khi thay $y_1 = y_o - at$ vào các đẳng thức

$$a_i(x_i^1 - x_i^o) - y_1 = y_o \ (i = 1,2,...,n) \text{ ta được}$$

$$x_i^1 = x_i^o + \frac{a}{a_i}t,\ i = 1, 2, ..., n.$$

Định lý được chứng minh.

3. Cách thực hành giải hệ phương trình (3)

Ta đặt

$$a_1x_1 + b_1 = a_2x_2 + b_2 = \dots = a_nx_n + b_n = y$$

Trước tiên ta xét

$$a_1x_1 + b_1 = a_2x_2 + b_2 = y.$$

Ta thấy rằng phương trình

$$a_1x_1 + b_1 = a_2x_2 + b_2$$

có nghiệm nguyên là

$$\begin{cases} x_1 = c_1 + a_2t_2, \\ x_2 = c_2 + a_1t_2 \end{cases}$$

với c_1, c_2 thỏa mãn $a_1c_1 + b_1 = a_2c_2 + b_2$ và t_2 là một số nguyên tùy ý.

Thay $x_1 = c_1 + a_2t_2$ vào biểu thức $y = a_1x_1 + b_1$ ta được

$$y = t_2^o + a_1a_2t,$$

trong đó $t_2^o = a_1c_1 + b_1$. Như vậy hệ phương trình (3) tương đương với hệ

$$\begin{cases} x_1 = c_1 + a_2t_2; \\ x_2 = c_2 + a_1t_2; \\ y = a_1a_2t_2 + t_2^o = a_3x_3 + b_3 = \dots = a_nx_n + b_n. \end{cases}$$

Ta xét

$$y = a_1a_2t_2 + t_2^o = a_3x_3 + b_3.$$

Vì a_1a_2 nguyên tố với a_3 nên phương trình

$$a_1a_2t_2 + t_2^o = a_3x_3 + b_3$$

có nghiệm nguyên là

$$\begin{cases} t_2 = d_1 + a_3t_3, \\ x_3 = d_2 + a_1a_2t_3, \end{cases}$$

với d_1, d_2 thỏa mãn $a_1a_2d_1 + t_2^0 = a_3d_2 + b_3$ và t_3 là một số nguyên tùy ý.

Thay $t_2 = d_1 + a_3t_3$ vào các biểu thức $y = a_1a_2t_2 + t_2^0$, $x_1 = c_1 + a_2t_2$ và $x_2 = c_2 + a_1t_2$ ta được

$$y = a_1a_2d_1 + t_2^0 + a_1a_2a_3t_3,$$
$$x_1 = a_2d_1 + c_1 + a_2a_3t_3,$$
$$x_2 = a_1d_1 + c_2 + a_1a_3t_3.$$

Do đó hệ phương trình (3) tương đương với hệ

$$x_1 = (a_2d_1 + c_1) + a_2a_3t_3,$$
$$x_2 = (a_1d_1 + c_2) + a_1a_3t_3,$$
$$x_3 = d_2 + a_1a_2t_3,$$
$$y = t_3^0 + a_1a_2a_3t_3 = a_4x_4 + b_4 = \dots = a_nx_n +$$
$+ b_n$, trong đó $t_3^0 = a_1a_2d_1 + t_2^0$.

Cứ tiếp tục tiến hành như thế sau $n-1$ bước ta đi đến

$$y = t_n^0 + a_1a_2\dots a_nt$$

và ta được nghiệm của hệ phương trình (3) là

$$\begin{cases} x_1 = x_1^0 + \dfrac{a}{a_1}t, \\ x_2 = x_2^0 + \dfrac{a}{a_2}t, \\ \dots\dots\dots \\ x_n = x_n^0 + \dfrac{a}{a_n}t, \end{cases}$$

trong đó t_n^0, x_1^0, x_2^0, ..., x_n^0 là những số nguyên xác định còn t là một số nguyên tùy ý và $a = a_1a_2\dots a_n$.

Ví dụ. Tìm tất cả nghiệm nguyên của hệ phương trình

$$3x_1 + 2 = 5x_2 + 3 = 7x_3 + 2$$

Trước hết ta xét $y = 3x_1 + 2 = 5x_2 + 3$. Ta có

$$\begin{cases} x_1 = 2 + 5t_2 \\ x_2 = 1 + 3t_2,\ t_2 \in \mathbf{Z} \end{cases}$$

là nghiệm của phương trình

$$3x_1 + 2 = 5x_2 + 3.$$

Từ đó ta có $y = 3x_1 + 2 = 3(2 + 5t_2) + 2 = 15t_2 + 8$ nên hệ phương trình đã cho tương đương với hệ

$$\begin{cases} x_1 = 2 + 5t_2. \\ x_2 = 1 + 3t_2. \\ y = 15t_2 + 8 = 7x_3 + 2. \end{cases}$$

Ta lại xét $y = 15t_2 + 8 = 7x_3 + 2$. Ta thấy phương trình $15t_2 + 8 = 7x_3 + 2$ có nghiệm nguyên là

$$\begin{cases} t_2 = 1 + 7t, \\ x_3 = 3 + 15t. \text{ với } t \in \mathbf{Z}. \end{cases}$$

Từ đó ta có

$$y = 15t_2 + 8 = 15(1 + 7t) + 8 = 23 + 105t,$$
$$x_1 = 2 + 5(1 + 7t) = 7 + 35t.$$
$$x_2 = 1 + 3(1 + 7t) = 4 + 21t.$$

Vậy hệ phương trình đã cho có các nghiệm nguyên là

$$\begin{cases} x_1 = 7 + 35t. \\ x_2 = 4 + 21t, \\ x_3 = 3 + 15t, \end{cases}$$

với t là một số nguyên tùy ý.

4. Chú ý. a) Từ điều kiện các số nguyên $a_1, a_2, \ldots, a_n$ là nguyên tố cùng nhau từng đôi một ta đã chứng minh được sự tồn tại của nghiệm nguyên của hệ phương trình (3) và đưa ra cách thực hành tìm các nghiệm nguyên của nó. Sau này (bài thứ bảy) chúng ta sẽ tìm được điều kiện có nghiệm nguyên và cách thực hành tìm các nghiệm nguyên của một hệ phương trình bậc nhất

$$a_1x_1 + b_1 = a_2x_2 + b_2 = \ldots = a_nx_n + b_n,$$

trong đó $a_1, a_2, \ldots, a_n$ và $b_1, b_2, \ldots, b_n$ là những số nguyên tùy ý cho trước.

b) Sau khi chứng minh định lý Trung Hoa về thặng dư ta suy ra rằng nếu cho trước n số nguyên khác 0 đôi một nguyên tố cùng nhau $a_1, a_2, ..., a_n$ và n số tự nhiên $b_1, b_2, ..., b_n$ thì ắt có những số nguyên mà khi chia chúng cho $a_1, a_2, ..., a_n$ được lần lượt các số dư là $b_1, b_2, ..., b_n$.

Chẳng hạn sau khi giải hệ phương trình

$$3x_1 + 2 = 5x_2 + 3 = 7x_3 + 2$$

ta cũng suy ra được rằng tất cả những số nguyên y có dạng

$$y = 23 + 105t, \; t \in z$$

khi chia cho 3, 5, 7 sẽ được lần lượt các sò dư là 2, 3, 2.

§2. PHƯƠNG TRÌNH BẬC HAI NHIỀU ẨN

I – PHƯƠNG TRÌNH BẬC HAI HAI ẨN DẠNG $X^2 - AY^2 = 1$.

Chúng ta xét phương trình bậc hai hai ẩn

$$x^2 - Ay^2 = 1 \qquad (1)$$

trong đó A là một số nguyên dương cho trước không là chính phương. Một phương trình như thế được gọi là *phương trình Pell*, chẳng hạn $x^2 - 2y^2 = 1$ là một phương trình Pell.

Phương trình (1) có nghiệm nguyên tầm thường là $x = 1$, $y = 0$, hơn nữa nếu phương trình (1) có nghiệm nguyên là x, y thì nhất thiết $x \neq 0$ cho nên vấn đề đặt ra là hãy nghiên cứu các nghiệm nguyên x, y không tầm thường của phương trình (1) với giả thiết $x > 0$, $y > 0$.

1. Nghiệm nguyên nhỏ nhất của phương trình (1). Giả sử phương trình (1) có nghiệm nguyên không tầm thường (*). Ta gọi nghiệm nguyên không tầm thường x_1, y_1 của phương trình (1) là nghiệm nguyên *nhỏ nhất* của phương trình (1) nếu như $x_1 + \sqrt{A}\, y_1$ là số nhỏ nhất trong tập hợp

$$M = \{ x + \sqrt{A}\, y \mid x, y \in Z, x > 0, y > 0, x^2 - Ay^2 = 1 \}.$$

(*) Về sau ta đã chứng minh được rằng phương trình (1) luôn luôn có nghiệm nguyên không tầm thường $x > 0$, $y > 0$.

Ví dụ: Bằng cách thử ta thấy $x = 3$, $y = 2$ là nghiệm nguyên nhỏ nhất của phương trình $x^2 - 2y^2 = 1$.

Từ định nghĩa ta suy ra rằng nghiệm nguyên nhỏ nhất (nếu có) của phương trình (1) là duy nhất.

Thật vậy, nếu x_1, y_1 và x'_1, y'_1 là hai nghiệm nguyên nhỏ nhất của phương trình (1) thì ta có

$x_1 + \sqrt{A} y_1 \leqslant x'_1 + \sqrt{A}\, y'_1$ và $x'_1 + \sqrt{A}\, y'_1 \leqslant x_1 + \sqrt{A}\, y_1$ cho nên suy ra

$$x_1 + \sqrt{A}\, y_1 = x'_1 + \sqrt{A}\, y'_1$$

hay là

$$x_1 - x'_1 = \sqrt{A}\,(y'_1 - y_1).$$

Từ đẳng thức sau cùng này ta suy ra rằng nếu $x_1 - x'_1$ là một số nguyên khác 0 thì $y'_1 - y_1$ cũng là một số nguyên khác 0 nên $\sqrt{A}\,(y'_1 - y_1)$ là một số vô tỷ, đây là điều không thể có được. Vậy $x'_1 = x_1$ và cũng từ đẳng thức sau cùng ở trên ta suy ra $y'_1 = y_1$.

2. Tập hợp nghiệm nguyên của phương trình (1)

a) Bổ đề 1. *Giả sử* x_0, y_0 *là một nghiệm nguyên của phương trình* (1) *và* n *là một số nguyên dương. Khi ấy tồn tại cặp số nguyên* x_n, y_n *sao cho*

$$x_n + \sqrt{A}\, y_n = (x_0 + \sqrt{A}\, y_0)^n$$
$$x_n - \sqrt{A}\, y_n = (x_0 - \sqrt{A}\, y_0)^n$$

và x_n, y_n *cũng là nghiệm của phương trình* (1).

Chứng minh. Áp dụng công thức nhị thức Niutơn ta có

$$(x_0 + \sqrt{A} y_0)^n = x_0^n + C_n^1 x_0^{n-1} \sqrt{A}\, y_0 + C_n^2\, x_0^{n-2} (\sqrt{A})^2 \times$$
$$\times\ y_0^2 + \ldots C_n^{n-1} x_0 (\sqrt{A})^{n-1} y_0^{n-1} + (\sqrt{A})^n y_0^n. \qquad (2)$$

Trong vế phải của đẳng thức (2), ta thấy rằng các số hạng thứ chẵn của tổng là những số nguyên nên tổng của các số hạng ấy là một số nguyên x_n, còn các số hạng thứ lẻ là tích của một số nguyên với $\sqrt{A}$ nên sau khi tách $\sqrt{A}$ ta có tổng của những số nguyên ấy là một số nguyên y_n, bởi vậy ta được

$$(x_o + \sqrt{A}\, y_o)^n = x_n + \sqrt{A}\, y_n.$$

Cũng trong đẳng thức (2) nếu thay $\sqrt{A}$ bởi $-\sqrt{A}$ ta sẽ được

$$(x_o - \sqrt{A}\, y_o)^n = x_n - \sqrt{A}\, y_n.$$

Bây giờ ta sẽ chứng minh cặp số nguyên x_n, y_n vừa xác định ở trên là nghiệm của phương trình (1).

Thật vậy ta có

$$x_n^2 - Ay_n^2 = (x_n + \sqrt{A}\, y_n)(x_n - \sqrt{A}\, y_n) =$$
$$= (x_o + \sqrt{A}\, y_o)^n (x_o - \sqrt{A}\, y_o)^n =$$
$$= (x_o^2 - Ay_o^2)^n.$$

Nhưng x_o, y_o là một nghiệm nguyên của phương trình (1) nghĩa là $x_o^2 - Ay_o^2 = 1$ cho nên từ đẳng thức

$$x_n^2 - Ay_n^2 = \left(x_o^2 - A\, y_o^2\right)^n$$

ta được $$x_n^2 - Ay_n^2 = 1.$$

Đẳng thức này chứng tỏ x_n, y_n nghiệm đúng phương trình (1).

b. Bổ đề 2. *Giả sử x_1, y_1 là nghiệm nguyên nhỏ nhất của phương trình (1) và x, y là một nghiệm tùy ý của phương trình (1) thế thì át có số nguyên dương n sao cho*

$$x + \sqrt{A}\, y = (x_1 + \sqrt{A}\, y_1)^n.$$

Chứng minh. Ta chứng minh bằng phương pháp phản chứng. Giả sử có một nghiệm nguyên x', y' sao cho

$$x' + \sqrt{A}\, y' \neq (x_1 + \sqrt{A}\, y_1)^n$$

với mọi số n nguyên dương.

Khi ấy bởi vì $x_1 \geqslant 1$, $y_1 \geqslant 1$ và $x_1 + \sqrt{A}\, y_1 > 1$ nên $x_1 + \sqrt{A}\, y_1$, $(x_1 + \sqrt{A}\, y_1)^2$, $(x_1 + \sqrt{A}\, y_1)^3$,... là một dãy sò dương tăng không bị chặn.

Theo giả thiết x_1, y_1 là nghiệm nguyên nhỏ nhất của phương trình (1) ta có

$$x' + \sqrt{A}\, y' > x_1 + \sqrt{A}\, y_1$$

bởi vậy từ giả thiết phản chứng ta suy ra rằng tồn tại số nguyên $m \geqslant 1$ sao cho

$$(x_1 + \sqrt{A}\, y_1)^m < x' + \sqrt{A}\, y' < (x_1 + \sqrt{A}\, y_1)^{m+1}. \quad (3)$$

Từ $(x_1 + \sqrt{A}\, y_1)\ (x_1 - \sqrt{A}\, y_1) = x_1^2 - Ay_1^2 = 1 > 0$ và $x_1 + \sqrt{A}\, y_1 > 0$, ta suy ra $x_1 - \sqrt{A}\, y_1 > 0$, cho nên sau khi nhân từng vế của các bất đẳng thức (3) với $(x_1 - \sqrt{A}\, y_1)^m > 0$ ta được $(x_1 + \sqrt{A}\, y_1)^m\ (x_1 - \sqrt{A}\, y_1)^m <$

$$(x' + \sqrt{A}\, y')\ (x_1 - \sqrt{A}\, y_1)^m < (x_1 + \sqrt{A}\, y_1)^{m+1}\ (x_1 - \sqrt{A}\, y_1)^m \quad (4)$$

Nhưng ta thấy rằng

$$(x_1 + \sqrt{A}\, y_1)^m\ (x_1 - \sqrt{A}\, y_1)^m = (x_1^2 - Ay_1^2)^m = 1$$

cho nên

$$(x_1 + \sqrt{A}\, y_1)^{m+1}\ (x_1 - \sqrt{A}\, y_1)^m = x_1 + \sqrt{A}\, y_1.$$

Hơn nữa theo bổ đề 1 giả sử x_m, y_m là cặp số nguyên thỏa mãn

$$(x_1 - \sqrt{A}\, y_1)^m = x_m - \sqrt{A}\, y_m,$$

ta sẽ có

$$(x' + \sqrt{A}\, y')\ (x_1 - \sqrt{A}\, y_1)^m = (x' + \sqrt{A}\, y')\ (x_m - \sqrt{A}\, y_m) =$$
$$= x'x_m - Ay'\, y_m + \sqrt{A}\, (y'x_m - x'y_m) = \overline{x} + \sqrt{A}\, \overline{y}.$$

trong đó $\overline{x} = x'x_m - Ay'y_m$ và $\overline{y} = y'x_m - x'y_m$ là những số nguyên.

Bởi vậy từ (4) chúng ta nhận được

$$1 < \overline{x} + \sqrt{A}\ \overline{y} < x_1 + \sqrt{A}\ y_1. \qquad (5)$$

Nếu như ta chứng minh được rằng cặp số nguyên $\overline{x}, \overline{y}$ là những số dương và nghiệm đúng phương trình (1) thì từ (5) ta sẽ dẫn đến mâu thuẫn bởi vì x_1, y_1 là nghiệm nguyên nhỏ nhất của phương trình (1) và khi ấy bổ đề 2 sẽ được chứng minh.

Rõ ràng cặp số nguyên $\overline{x}, \overline{y}$ nghiệm đúng phương trình (1). Thật vậy, trong đẳng thức xác định $\overline{x} + \sqrt{A}\ \overline{y}$ ở trên nếu ta thay $\sqrt{A}$ bởi $-\sqrt{A}$ thì từ

$$\overline{x} + \sqrt{A}\ \overline{y} = (x' + \sqrt{A}\ y')\ (x_1 - \sqrt{A}\ y_1)^m$$

ta sẽ có

$$\overline{x} - \sqrt{A}\ \overline{y} = (x' - \sqrt{A}\ y')\ (x_1 + \sqrt{A}\ y_1)^m$$

cho nên

$$\overline{x}^2 - A\ \overline{y}^2 = (\overline{x} + \sqrt{A}\ \overline{y})\ (\overline{x} - \sqrt{A}\ \overline{y}) =$$
$$= (x' + \sqrt{A}\ y')(x_1 - \sqrt{A}\ y_1)^m\ (x' - \sqrt{A}\ y')\ (x_1 - \sqrt{A}\ y_1)^m =$$
$$= (x'^2 - A\ y'^2)\ (x_1^2 - Ay_1^2)^m.$$

Nhưng x', y' và x_1, y_1 là hai nghiệm của phương trình (1) nên ta có $x'^2 - Ay'^2 = 1$ và $x_1^2 - Ay_1^2 = 1$ bởi vậy $\overline{x}^2 - A\overline{y}^2 = 1$, nói khác đi $\overline{x}, \overline{y}$ là một nghiệm của phương trình (1).

Ta còn phải chứng minh $\overline{x} > 0$ và $\overline{y} > 0$. Như ta đã nhận xét ở trên vì $\overline{x}, \overline{y}$ là nghiệm nguyên của phương trình (1) nên $\overline{x} \neq 0$, hơn nữa ta còn có $\overline{y} \neq 0$, bởi vì nếu $\overline{y} = 0$ thì $\overline{x}^2 = 1$, nhưng trong khi đó từ (5) ta lại có $\overline{x} > 1$ là điều vô lý. Mặt khác ta thấy $\overline{x}$ và $\overline{y}$ phải cùng dấu bởi vì nếu $\overline{x}$ và $\overline{y}$ trái dấu nhau thì $\overline{x}$ và $-\overline{y}$ là cùng dấu nên từ $\overline{x} + \sqrt{A}\ \overline{y} > 1$ ta có

$$|\overline{x} - \sqrt{A}\,\overline{y}| > \overline{x} + \sqrt{A}\,\overline{y} > 1,$$

trong khi đó

$$(\overline{x} + \sqrt{A}\,\overline{y})(\overline{x} - \sqrt{A}\,\overline{y}) = \overline{x}^2 - A\,\overline{y}^2 = 1$$

là điều vô lý.

Như vậy $\overline{x}$ và $\overline{y}$ là hai số nguyên khác 0 và cùng dấu với nhau cho nên từ bất đẳng thức $\overline{x} + \sqrt{A}\,\overline{y} > 1$ ta được $\overline{x} > 0$ và $\overline{y} > 0$. Đến đây bổ đề được chứng minh.

Từ hai bổ đề ở trên ta suy ra được định lý sau đây về tập hợp nghiệm nguyên của phương trình (1).

c) Định lý. *Nếu phương trình (1) có nghiệm nguyên nhỏ nhất x_1, y_1 thì tập hợp nghiệm nguyên của phương trình (1) gồm các cặp số nguyên $\pm x_n$, $\pm y_n$:*

$$\begin{cases} x_n = \dfrac{1}{2}\left((x_1 + \sqrt{A}\,y_1)^n + (x_1 - \sqrt{A}\,y_1)^n\right), \\ y_n = \dfrac{1}{2\sqrt{A}}\left((x_1 + \sqrt{A}\,y_1)^n - (x_1 - \sqrt{A}\,y_1)^n\right) \end{cases} \tag{6}$$

với n là một số tự nhiên tùy ý.

Chứng minh. Trước hết theo bổ đề 1 ta thấy rằng các số x_n, y_n xác định theo công thức (6) là những số nguyên và bằng cách thử ta được

$$(\pm x_n)^2 - A(\pm y_n)^2 = 1,$$

nghĩa là các cặp số nguyên $\pm x_n$, $\pm y_n$ là nghiệm của phương trình (1).

Bây giờ giả sử x, y là một nghiệm nguyên tùy ý của phương trình (1). Nếu x, y là nghiệm nguyên tầm thường của phương trình (1) thì ta có thể viết

$$\begin{cases} x = 1 = \dfrac{1}{2}\left((x_1 + \sqrt{A}\,y_1)^0 + (x_1 - \sqrt{A}\,y_1)^0\right), \\ y = 0 = \dfrac{1}{2\sqrt{A}}\left((x_1 + \sqrt{A}\,y_1)^0 - (x_1 - \sqrt{A}\,y_1)^0\right). \end{cases}$$

Nếu $x > 0$, $y > 0$ thì theo bổ đề 2 ắt có số nguyên dương n sao cho

$$x + \sqrt{A}\, y = (x_1 + \sqrt{A}\, y_1)^n$$

và khi ấy ta cũng có

$$x - \sqrt{A}\, y = (x_1 - \sqrt{A}\, y_1)^n.$$

Từ hai đẳng thức trên đây ta nhận được

$$\begin{cases} x = \dfrac{1}{2}\left((x_1 + \sqrt{A}\, y_1)^n + (x_1 - \sqrt{A}\, y_1)^n\right), \\ y = \dfrac{1}{2\sqrt{A}}\left((x_1 + \sqrt{A}\, y_1)^n - (x_1 - \sqrt{A}\, y_1)^n\right), \end{cases}$$

với n là một số nguyên dương.

Định lý chứng minh xong.

Ví dụ. Phương trình $x^2 - 2y^2 = 1$ có nghiệm nguyên nhỏ nhất là $x_1 = 3$, $y_1 = 2$ nên tập hợp nghiệm nguyên của phương trình này gồm tất cả các cặp số nguyên $\pm x_n$, $\pm y_n$ trong đó

$$x_n = \frac{1}{2}\left((3 + 2\sqrt{2})^n + (3 - 2\sqrt{2})^n\right),$$

$$y_n = \frac{1}{2\sqrt{2}}\left((3 + 2\sqrt{2})^n - (3 - 2\sqrt{2})^n\right)$$

với n là một số tự nhiên tùy ý.

Chẳng hạn với $n = 0$ ta được $x = \pm 1$, $y = 0$,
với $n = 1$ ta được $x = \pm 3$, $y = \pm 2$,
với $n = 2$ ta được $x = \pm 17$, $y = \pm 12$,...,.

3. Sự tồn tại nghiệm nguyên không tầm thường của phương trình (1)

Định lý. *Với A là một số nguyên dương bất kỳ không là chính phương, phương trình*

$$x^2 - A\, y^2 = 1 \qquad (1)$$

có nghiệm nguyên không tầm thường $x > 0$, $y > 0$.

Chứng minh. Khai triển $\sqrt{A}$ thành liên phân số, giả sử ta được

$$\sqrt{A} = [q_0 : (q_1, q_2, \ldots, q_n, 2q_0)],$$

Gọi $\frac{P_n}{Q_n}$ và $\frac{P_{n-1}}{Q_{n-1}}$ là hai giản phân thứ n và thứ n − 1 của liên phân số biểu diễn $\sqrt{A}$, ta có

$$\sqrt{A} = \frac{\alpha_{n+1} P_n + P_{n-1}}{\alpha_{n+1} Q_n + Q_{n-1}}, \qquad (7)$$

trong đó

$$\alpha_{n+1} = 2q_0 + \cfrac{1}{q_1 + \cfrac{1}{q_2 + \cdots}} = \sqrt{A} + q_0.$$

Trong đẳng thức (7) thay $\alpha_{n+1} = \sqrt{A} + q_0$ ta được $\sqrt{A}\,(\sqrt{A} + q_0) Q_n - \sqrt{A}\; Q_{n-1} = (\sqrt{A} + q_0) P_n + P_{n-1}$ hay là

$$A . Q_n - q_0 P_n - P_{n-1} = (P_n - q_0 Q_n - Q_{n-1}) . \sqrt{A}.$$

Nhưng $AQ_n - q_0P_n - P_{n-1}$ và $P_n - q_0 Q_n - Q_{n-1}$ là những số nguyên và $\sqrt{A}$ là một số vô tỷ nên đẳng thức trên đây cho ta $AQ_n - q_0 P_n - P_{n-1} = 0$ và $P_n - q_0\times$ $\times Q_n - Q_{n-1} = 0$ tức là

$$P_{n-1} = AQ_n - q_0 P_n.$$
$$Q_{n-1} = P_n - q_0 Q_n.$$

Từ tính chất của giản phân

$$P_n Q_{n-1} - Q_n P_{n-1} = (-1)^{n-1}$$

ta được

$$P_n(P_n - q_0 Q_n) - Q_n (AQ_n - q_0 P_n) = (-1)^{n-1}$$

hay là
$$P_n^2 - AQ_n^2 = (-1)^{n-1}. \qquad (8)$$

Nếu n là số lẻ ta có

$$P_n^2 - A\, Q_n^2 = 1$$

nghĩa là P_n, Q_n là một nghiệm nguyên dương của phương trình (1).

Nếu n là số chẵn thì lặp lại lí luận như ở trên bằng cách chỗ nào là n thì thay bởi 2n + 1 ta sẽ đi đến

$$P_{2n+1}^2 - AQ_{2n+1}^2 = (-1)^{2n}$$

hay là

$$P_{2n+1}^2 - AQ_{2n+1}^2 = 1.$$

Nói khác đi, trong trường hợp này P_{2n+1}, Q_{2n+1} là một nghiệm nguyên dương của phương trình (1).

Định lý đã được chứng minh.

Người ta cũng chứng minh được rằng mỗi một nghiệm nguyên dương của phương trình (1) đều là tử số và mẫu số của một giản phân của liên phân số biểu diễn $\sqrt{A}$. Hơn nữa người ta cũng chứng minh được rằng nếu n là số tự nhiên xác định như ở cách chứng minh định lý trên đây thì ta có $x = P_n$, $y = Q_n$ hoặc $x = P_{2n+1}$, $y = Q_{2n+1}$ là nghiệm nguyên nhỏ nhất của phương trình (1) tùy theo n là số lẻ hoặc n là số chẵn.

4. Các ví dụ

Ví dụ 1. Tìm các nghiệm nguyên của phương trình

$$x^2 - 11y^2 = 1.$$

Khai triển $\sqrt{11}$ thành liên phân số ta được

$$\sqrt{11} = [3; (3, 6)].$$

n = 1 là một số lẻ nên ta có $x_1 = P_1 = 10$ và $y_1 = Q_1 = 3$ là nghiệm nguyên nhỏ nhất của phương trình $x^2 - 11y^2 = 1$, do đó nghiệm nguyên của nó gồm tất cả các cặp số nguyên $\pm x_n$, $\pm y_n$, trong đó

$$\begin{cases} x_n = \dfrac{1}{2}\left((10 + 3\sqrt{11})^n + (10 - 3\sqrt{11})^n\right), \\ y_n = \dfrac{1}{2\sqrt{11}}\left((10 + 3\sqrt{11})^n - (10 - 3\sqrt{11})^n\right) \end{cases}$$

với n là một số tự nhiên tùy ý.

Ví dụ 2. Tìm nghiệm nguyên dương nhỏ nhất của phương trình

$$x^2 - 29y^2 = 1.$$

Khai triển $\sqrt{29}$ thành liên phân số ta được

$$\sqrt{29} = [5; (2, 1, 1, 2, 10)].$$

Ở đây n = 4 là một số chẵn nên ta có $x_1 = P_9 = 9801$, $y_1 = Q_9 = 1820$ là nghiệm nguyên nhỏ nhất của phương trình $x^2 - 29y^2 = 1$.

5. Các trường hợp đặc biệt của phương trình $x^2 - Ay^2 = 1$.

Ta đã giải quyết được việc tìm nghiệm nguyên của phương trình $x^2 - Ay^2 = 1$ với A là một số nguyên dương và $\sqrt{A}$ là một số vô tỉ. Bây giờ ta xét các trường hợp đặc biệt của phương trình $x^2 - Ay^2 = 1$.

a) Trường hợp $A > 0$ và $\sqrt{A}$ là một số nguyên.

Đặt $\sqrt{A} = \alpha$ ta viết phương trình $x^2 - Ay^2 = 1$ dưới dạng

$$(x - \alpha y)(x + \alpha y) = 1.$$

Bởi vì α là một số nguyên cho nên điều kiện cần và đủ để cặp số nguyên x_o, y_o nghiệm đúng phương trình $(x - \alpha y)(x + \alpha y) = 1$ là $x_o + \alpha y_o$ và $x_o - \alpha y_o$ cùng bằng 1 hoặc cùng bằng -1. Từ đó suy ra $x_o = 1$, $y_o = 0$ hoặc là $x_o = -1$, $y_o = 0$. Như vậy với $\sqrt{A} = \alpha$ là một số nguyên thì phương trình $x^2 - Ay^2 = 1$ chỉ có hai nghiệm nguyên là $x = 1$, $y = 0$, và $x = -1$, $y = 0$.

b) Trường hợp A là một số nguyên âm.

Nếu $A = -1$ thì phương trình $x^2 - Ay^2 = 1$ sẽ là $x^2 + y^2 = 1$ cho nên nó chỉ có bốn nghiệm nguyên là $x = \pm 1$, $y = 0$ và $x = 0$, $y = \pm 1$.

Nếu A là một số nguyên âm khác -1 thì phương trình $x^2 - Ay^2 = 1$ chỉ có hai nghiệm nguyên duy nhất là $x = \pm 1$, $y = 0$.

II – PHƯƠNG TRÌNH BẬC HAI BA ẨN DẠNG $X^2+Y^2=Z^2$.

1. Chúng ta đặt vấn đề nghiên cứu các nghiệm nguyên của phương trình bậc hai ba ẩn

$$x^2 + y^2 = z^2 \qquad (9)$$

với $x > 0$, $y > 0$, $z > 0$.

Về mặt hình học, các số nguyên dương $\overline{x, y}$, z nghiệm đúng phương trình (9) biểu thị độ dài các cạnh của một tam giác vuông, bởi vậy nghiệm nguyên dương của phương trình (9) được gọi là các số *Pitago*.

Trước hết ta thấy rằng nếu các số nguyên x, y, z nghiệm đúng phương trình (9) thì mọi hệ ba số nguyên xt, yt, zt cũng nghiệm đúng phương trình (9). Ngược lại nếu các số nguyên xt, yt, zt nghiệm đúng phương trình (9) (với t là một số nguyên khác 0) thì x, y, z cũng nghiệm đúng phương trình (9). Bởi vậy ta có thể giả thiết chỉ xét các nghiệm nguyên dương x, y, z của phương trình (9) với $(x, y, z) = 1$.

Chúng ta chú ý rằng từ điều kiện x, y, z là nguyên tố cùng nhau và $x^2 + y^2 = z^2$ ta suy ra x, y, z là nguyên tố cùng nhau từng đôi một. Thật vậy, chẳng hạn nếu $(x, y) = d > 1$, thì d^2 là ước của z^2 nên d là ước của z, từ đó lại có $(x, y, z) > 1$. Bây giờ chúng ta chứng minh định lý về tập hợp nghiệm nguyên của phương trình (9).

2. Định lý. *Các số nguyên dương nguyên tố cùng nhau x, y, z là nghiệm của phương trình*

$$x^2 + y^2 = z^2 \qquad (9)$$

khi và chỉ khi một trong hai số x hoặc y có dạng 2mn số kia có dạng $m^2 - n^2$ và z có dạng $m^2 + n^2$ với m, n là hai số nguyên dương nguyên tố cùng nhau, $m > n$ và chẵn lẻ khác nhau.

Chứng minh. a) Giả sử x, y, z là những số nguyên dương nguyên tố cùng nhau nghiệm đúng phương trình (9) nghĩa là ta có đẳng thức

$$x^2 + y^2 = z^2.$$

Khi ấy vì ta có $(x, y) = 1$ nên không thể xảy ra x và y cùng là số chẵn; thậm chí cũng không thể xảy ra x và y cùng là số lẻ, thật vậy nếu $x = 2k + 1$ và $y = 2l + 1$ thì $$z^2 = x^2 + y^2 = 4(k^2 + l^2 + k + l) + 2$$
là điều vô lý bởi vì bình phương của một số khi chia cho 4 không thể dư là 2 được.

Vậy trong hai số x và y phải có một số là chẵn một số là lẻ. Giả sử x là số chẵn, lúc ấy từ đẳng thức $x^2 + y^2 = z^2$ ta có y và z là các số lẻ và

$$\left(\frac{x}{2}\right)^2 = \frac{z + y}{2} \cdot \frac{z - y}{2},$$

trong đó $\left(\frac{z + y}{2}, \frac{z - y}{2}\right) = 1$ bởi vì $(z, y) = 1$.

Nhưng khi tích của hai số nguyên tố cùng nhau là một chính phương thì mỗi nhân tử phải là một chính phương, cho nên ắt có các số nguyên dương m, n sao cho $$\frac{z + y}{2} = m^2, \quad \frac{z - y}{2} = n^2.$$

Từ đó ta được

$$x = 2mn, \; y = m^2 - n^2, \; z = m^2 + n^2.$$

Do $\frac{x + y}{2} = m^2$ và $\frac{z - y}{2} = n^2$ là hai số nguyên tố cùng nhau nên m và n là nguyên tố cùng nhau và $m > n > 0$. Hơn nữa từ y và z là hai số lẻ ta còn có m và n là hai số chẵn lẻ khác nhau.

b) Bây giờ giả sử m và n là hai số nguyên dương chẵn lẻ khác nhau, nguyên tố cùng nhau và $m > n$.

Ta phải chứng minh rằng ba số $x = 2mn$, $y = m^2 - n^2$, $z = m^2 + n^2$ là những số nguyên dương nguyên tố cùng nhau và là một nghiệm của phương trình (9).

Thật vậy, rõ ràng ba số x, y, z xác định như vậy là những số nguyên dương, nghiệm đúng phương trình (9), bởi vì chúng ta có đẳng thức

$$(2mn)^2 + (m^2 - n^2)^2 = (m^2 + n^2)^2.$$

Mặt khác do m, n là hai số nguyên dương chẵn lẻ khác nhau nên $y = m^2 - n^2$ và $z = m^2 + n^2$ phải là những số lẻ. Hơn nữa ta có $(y, z) = 1$ bởi vì nếu như $(y, z) = d > 1$ thì ta cũng có

$$\left(\frac{z + y}{2}, \frac{z - y}{2}\right) = d > 1$$

tức là

$$(m^2, n^2) = d > 1,$$

điều đó không thể xảy ra được với $(m, n) = 1$.

Vậy $(y, z) = 1$ và do đó $(x, y, z) = 1$. Định lý được chứng minh. Từ định lý này và nhận xét khởi đầu ta có hệ quả sau đây.

3. Hệ quả. *Phương trình*

$$x^2 + y^2 = z^2$$

có nghiệm nguyên là và chỉ là các bộ ba số nguyên x, y, z xác định như sau:

$$\begin{cases} x = \pm 2mnt \ (\text{hoặc } x = \pm (m^2 - n^2)t, \\ y = \pm (m^2 - n^2)t \ (\text{hoặc } y = \pm 2mnt), \\ z = \pm (m^2 + n^2)t \end{cases}$$

với m, n, t là những số nguyên tùy ý thỏa mãn điều kiện $m > n > 0$, $(m, n) = 1$ và mn chẵn.

Ví dụ. Với $t = 2$, $m = 7$, $n = 4$ chúng ta được

$$x = \pm 112, \ y = \pm 66, \ z = \pm 130$$

hoặc

$$x = \pm 66, \ y = \pm 112, \ z = \pm 130.$$

§ 3. PHƯƠNG TRÌNH $x^n + y^n = z^n$

Sau khi nghiên cứu nghiệm nguyên của phương trình bậc hai ba ẩn dạng

$$x^2 + y^2 = z^2$$

chúng ta có thể đặt vấn đề nghiên cứu nghiệm nguyên của phương trình bậc hai ba ẩn

$$ax^2 + by^2 = cz^2$$

với a, b, c là những số nguyên cho trước. Trong tiết này chúng ta đặt vấn đề nghiên cứu nghiệm nguyên của phương trình

$$x^n + y^n = z^n$$

với n là một số tự nhiên lớn hơn 2.

Nhà toán học Pháp nổi tiếng Phécma đã khẳng định rằng *với số tự nhiên $n > 2$, phương trình*

$$x^n + y^n = z^n \qquad (1)$$

không có nghiệm nguyên dương.

Cho đến nay mệnh đề do Phécma nêu lên (gọi là *định lý lớn Phécma* hay là *bài toán Phécma*) vẫn chưa được giải quyết triệt để.

Nếu điều khẳng định của Phécma đúng với n thì nó cũng đúng với kn (bởi vì phương trình $x^{kn} + y^{kn} = z^{kn}$ có thể viết dưới dạng $(x^k)^n + (y^k)^n = (z^k)^n$), bởi vậy chỉ cần chứng minh định lý Phécma với các số mũ nguyên tố $p \geqslant 3$ và với $n = 4$ là đủ.

Ơle đã chứng minh định lý Phécma đúng với $n = 3$ và $n = 4$. Điriclê và Lơgiăngđrơ đã chứng minh định lý Phécma đúng với $n = 5$. Lamơ đã chứng minh định lý Phécma đúng với $n = 7$. Kyme đã dùng lý thuyết số đại số để giải bài toán Phécma, ông đã chứng minh định lý Phécma đúng với tất cả các giá trị $n \leqslant 100$. Đến năm 1956, bằng máy tính điện tử, người ta đã chứng minh được định lý Phécma đúng với tất cả các số mũ nguyên tố $n < 4003$.

Sau đây chúng ta nêu lên một cách chứng minh định lý Phécma với n = 4, bằng phương pháp sơ cấp dựa vào công thức nghiệm nguyên dương của phương trình $x^2 + y^2 = z^2$.

1. Phương trình

$$x^4 + y^4 = z^4 \qquad (2)$$

không có nghiệm nguyên dương.

Chứng minh. a) Để chứng minh định lý, đầu tiên ta chứng minh rằng phương trình

$$x^4 + y^4 = z^2 \qquad (3)$$

không có nghiệm nguyên dương.

Thật vậy, giả sử trái lại rằng phương trình (3) có nghiệm nguyên dương x_o, y_o, z_o. Khi ấy nếu x_o, y_o có ước chung lớn nhất là $d > 1$ thì rõ ràng d^2 là ước của z_o và đẳng thức

$$\left(\frac{x_o}{d}\right)^4 + \left(\frac{y_o}{d}\right)^4 = \left(\frac{z_o}{d^2}\right)^2$$

chứng tỏ rằng $\frac{x_o}{d}$, $\frac{y_o}{d}$, $\frac{z_o}{d^2}$ là một nghiệm nguyên dương của phương trình (3) với $\frac{x_o}{d}$ và $\frac{y_o}{d}$ là nguyên tố cùng nhau. Vì vậy bằng cách ký hiệu lại, ta có thể giả thiết là ta đang xét nghiệm nguyên dương x_o, y_o, z_o nguyên tố cùng nhau (do x_o, y_o nguyên tố cùng nhau).

Từ đẳng thức

$$\left(x_o^2\right)^2 + \left(y_o^2\right)^2 = z_o^2$$

và từ công thức nghiệm nguyên dương của phương trình

$$x^2 + y^2 = z^2$$

ta suy ra rằng (vai trò x_o và y_o như nhau, nên ta có thể giả thiết x_o là số chẵn, do đó y_o là số lẻ)

$$x_0^2 = 2mn,\ y_0^2 = m^2 - n^2,\ z_0 = m^2 + n^2,$$

trong đó $m > n > 0$, $(m, n) = 1$, mn chẵn.

Từ đẳng thức

$$y_0^2 + n^2 = m^2, \qquad (4)$$

vì y_0 là số lẻ, ta phải có n là số chẵn (và do đó m là số lẻ) chẳng hạn $n = 2n'$ với n' là một số nguyên dương. Khi ấy ta có

$$\left(\frac{x_0}{2}\right)^2 = mn',$$

trong đó $(m, n') = 1$ (bởi vì $(m, n) = 1$).

Như lý luận ở 2.II, § 2, ta có các số nguyên z_1, n_1 sao cho

$$m = z_1^2,\ n' = n_1^2$$

trong đó $(z_1, n_1) = 1$ và z_1 là một số lẻ (bởi vì m là số lẻ). Thay các giá trị của m và $n = 2n'$ vào đẳng thức (4) ta được

$$y_0^2 + (2n_1^2)^2 = z_1^4$$

trong đó $(2n_1^2, y_0) = 1$ (bởi vì $(2n_1^2, z_1^2) = (2n', m) =$
$= (n, m) = 1$).

Lại áp dụng kết quả ở 2.II § 2 với đẳng thức

$$y_0^2 + (2n_1^2)^2 = (z_1^2)^2$$

ta suy ra

$$2n_1^2 = 2uv,\ z_1^2 = u^2 + v^2$$

trong đó $u > v > 0$, $(u, v) = 1$ và uv chẵn.

Nhưng u, v là những số nguyên dương nguyên tố cùng nhau nên từ đẳng thức

$$n_1^2 = uv$$

ta suy ra rằng tồn tại các số nguyên dương x_1, y_1 sao cho

$$u = x_1^2, \ v = y_1^2.$$

Khi ấy từ đẳng thức

$$z_1^2 = u^2 + v^2$$

ta được

$$x_1^4 + y_1^4 = z_1^2.$$

Đẳng thức sau cùng này chứng tỏ x_1, y_1, z_1 là một nghiệm nguyên dương của phương trình (3), trong đó ta dễ ý rằng

$$z_1 \leqslant z_1^2 = m < m^2 < z_o$$

tức là $z_1 < z_o$. Hơn nữa từ $u = x_1^2$, $v = y_1^2$ là nguyên tố cùng nhau ta suy ra rằng x_1, y_1 cũng là nguyên tố cùng nhau và do đó x_1, y_1, z_1 cũng là ba số nguyên dương nguyên tố cùng nhau.

Như vậy, từ giả thiết về sự tồn tại một nghiệm nguyên dương x_o, y_o, z_o với $(x_o, y_o, z_o) = 1$ của phương trình (3) ta lại suy ra sự tồn tại một nghiệm nguyên dương x_1, y_1, z_1 của phương trình ấy với $(x_1, y_1, z_1) = 1$ và $z_1 < z_o$.

Áp dụng lập luận trên ta lại suy ra sự tồn tại một nghiệm nguyên dương x_2, y_2, z_2 của phương trình (3) với $(x_2, y_2, z_2) = 1$ và $z_2 < z_1$.

Quá trình này có thể lặp lại vô số lần, bởi vậy với $k = 0$, $k = 1$, $k = 2$, ... ta tìm được một nghiệm nguyên dương x_k, y_k, z_k với $(x_k, y_k, z_k) = 1$ và $z_{k+1} < z_k$ của phương trình

$$x^4 + y^4 = z^2.$$

Điều này vô lý, vì không thể tồn tại vô số số nguyên dương z_o, z_1, z_2, ... thỏa mãn.

$$z_o > z_1 > z_2 > \dots$$

Điều vô lý này chứng tỏ phương trình (3) không có nghiệm nguyên dương.

b) Bây giờ chứng minh rằng phương trình

$$x^4 + y^4 = z^4 \quad (2)$$

không có nghiệm nguyên dương

Thật vậy, giả sử trái lại rằng phương trình (2) có nghiệm nguyên dương là x_0, y_0, z_0. Khi ấy ta có x_0, y_0, z_0^2 là một nghiệm nguyên dương của phương trình

$$x^4 + y^4 = z^2$$

là điều mâu thuẫn với kết quả đã chứng minh ở trên. Vậy phương trình $x^4 + y^4 = z^4$ không có nghiệm nguyên dương.

Định lý đã được chứng minh.

2. Sự không có nghiệm nguyên khác không của phương trình

$$x^3 + y^3 = z^3. \quad (4)$$

Để chứng minh rằng phương trình $x^4 + y^4 = z^4$ không có nghiệm nguyên dương ta đã dựa vào công thức nghiệm nguyên dương của phương trình $x^2 + y^2 = z^2$. Bằng cách dựa vào công thức nghiệm nguyên của phương trình $x^2 + 3y^2 = z^3$ người ta có thể chứng minh được rằng phương trình $x^3 + y^3 = z^3$ không có nghiệm nguyên khác không.

Trước hết ta nêu lên một kết quả mà người ta đã tìm được như sau. (Phép chứng minh kết quả này vượt ra ngoài khuôn khổ của cuốn sách này).

Bộ ba số nguyên x, y, z, trong đó x và y nguyên tố cùng nhau và z là số lẻ là nghiệm của phương trình

$$x^2 + 3y^2 = z^3$$

khi và chỉ khi

$$\begin{cases} x = m(m^2 - 9n^2), \\ y = 3n(m^2 - n^2), \\ z = m^2 + 3n^2 \end{cases} \quad (5)$$

với m và n là những số nguyên tùy ý.

Bây giờ ta chứng minh sự không tồn tại nghiệm khác không của (4).

Thật vậy, giả sử trái lại rằng phương trình (4) có nghiệm nguyên khác không là x_0, y_0, z_0, ta có đẳng thức

$$x_0^3 + y_0^3 = z_0^3. \tag{6}$$

Giả sử $d > 1$ là ước chung lớn nhất của hai số bất kỳ trong ba số x_0, y_0, z_0, thì d cũng là ước của số còn lại và ta có đẳng thức

$$\left(\frac{x_0}{d}\right)^3 + \left(\frac{y_0}{d}\right)^3 = \left(\frac{z_0}{d}\right)^3.$$

Điều đó chứng tỏ $\frac{x_0}{d}$, $\frac{y_0}{d}$, $\frac{z_0}{d}$ cũng là một nghiệm nguyên khác không của phương trình (4) mà các giá trị đó nguyên tố cùng nhau từng đôi một. Vì vậy bằng cách ký hiệu lại, ta có thể giả thiết là ta đang xét các nghiệm nguyên khác không x_0, y_0, z_0 của phương trình (4) với x_0, y_0, z_0 nguyên tố cùng nhau từng đôi một (và do đó nguyên tố cùng nhau). Từ đó hai trong ba số x_0, y_0, z_0, là lẻ, số còn lại là chẵn. Ta giả thiết hai số x_0, y_0 ở vế trái của đẳng thức (6) là lẻ. Giả thiết này không làm mất tính tổng quát vì khi một trong hai số này là chẵn, chẳng hạn x_0, thì ta lại có đẳng thức

$$(-y_0)^3 + z_0^3 = x_0^3$$

cùng dạng với đẳng thức (6) trong đó cả hai số ở cùng một vế là lẻ.

Từ giả thiết x_0, y_0 là hai số lẻ ta có

$$x_0 + y_0 = 2p,\ x_0 - y_0 = 2q,$$

trong đó p, q là những số nguyên khác không. Khi ấy vì $x_0 = p + q$, $y_0 = p - q$ nên p và q phải nguyên tố cùng nhau và một trong chúng là lẻ còn số kia là chẵn.

Đẳng thức (6) có thể viết dưới dạng

$$(x_0 + y_0)\left(\left(\frac{x_0 + y_0}{2}\right)^2 + 3\left(\frac{x_0 - y_0}{2}\right)\right)^2 = z_0^3$$

nên ta có

$$2p(p^2 + 3q^2) = z_0^3. \tag{7}$$

Từ đẳng thức này do z_0 là chẵn ta có p là chẵn (do đó q là lẻ) và $p^2 + 3q^2$ là lẻ. Nhưng p và q nguyên tố cùng nhau nên p và $p^2 + 3q^2$ có ước chung lớn nhất hoặc là 1 hoặc là 3. Chúng ta hãy xét từng trường hợp đó.

Giả sử rằng p và p^2+3q^2 có ước chung lớn nhất là 1 Khi ấy dĩ nhiên p không chia hết cho 3. Từ đẳng thức (7) và do $(2p, p^2 + 3q^2) = 1$ ta suy ra rằng ắt có hai số nguyên khác không r và s sao cho

$$2p = r^3,\ p^2 + 3q^2 = s^3.$$

Theo nhận xét khởi đầu, từ đẳng thức $p^2 + 3q^2 = s^3$ ta suy ra rằng p, q, s phải có dạng như ở công thức (5), nghĩa là có các số nguyên m, n sao cho

$$p = m(m^2 - 9n^2),\ q = 3n(m^2 - n^2),\ s = m^2 + 3n^2.$$

Bởi vì q là số lẻ nên ta phải có n là lẻ và m là chẵn không chia hết cho 3. Hơn nữa $(m, n) = 1$ (do $(p, q) = 1$). Từ hai giá trị của p ở trên chúng ta có đẳng thức

$$2m(m + 3n)(m - 3n) = r^3. \tag{8}$$

Do m là số chẵn không chia hết cho 3 và n là số lẻ, $2m$, $m + 3n$, $m - 3n$ là những số nguyên tố cùng nhau từng đôi một, bởi vậy từ đẳng thức (8) ta suy ra rằng tồn tại các số nguyên khác không x_1, y_1, z_1 sao cho

$$m + 3n = x_1^3,\ m - 3n = y_1^3,\ 2m = z_1^3.$$

Từ các đẳng thức này ta được

$$x_1^3 + y_1^3 = z_1^3$$

nói khác đi x_1, y_1, z_1 là nghiệm nguyên khác không của phương trình (4) với $(x_1, y_1, z_1) = 1$.

Ta dễ ý thấy rằng

$$|x_1| \leqslant |x_1^3| \leqslant |p| < |2p| < |x_o|$$

tức là

$$|x_1| < |x_o|.$$

Bây giờ ta xét trường hợp p và $p^2 + 3q^2$ có ước chung lớn nhất là 3. Khi ấy ta viết $p = 3t$. Từ đẳng thức (7) ta có

$$6t = 9r^3,\ 9t^2 + 3q^2 = 3s^2$$

hay là

$$2t = 3r^3,\ q^2 + 3t^2 = s^3,$$

trong đó ta thấy t là số chẵn do đó q là số lẻ.

Từ đẳng thức $q^2 + 3t^2 = s^3$, theo nhận xét khởi đầu ta suy ra rằng q, t, s có dạng như ở công thức (5), nghĩa là ắt có các số nguyên m, n sao cho

$$q = m(m^2 - 9n^2),\ t = 3n(m^2 - n^2),\ s = m^2 + 3n^2.$$

Bởi vì t là số chẵn nên n là số chẵn và m là số lẻ. Từ hai giá trị của t ở trên chúng ta có

$$6n(m^2 - n^2) = 3r^3$$

hay là

$$2n(m + n)(m - n) = r^3. \quad (9)$$

Rõ ràng 2n, m + n, m − n là những số nguyên tố cùng nhau từng đôi một nên từ đẳng thức (9) ta suy ra rằng tồn tại các số nguyên khác không x_1, y_1, z_1 sao cho

$$m + n = x_1^3,\ m - n = y_1^3,\ 2n = z_1^3.$$

Từ các đẳng thức sau cùng này ta được

$$x_1^3 + y_1^3 = z_1^3$$

nói khác đi x_1, y_1, z_1 cũng là nghiệm nguyên khác không của phương trình (4) với $(x_1, y_1, z_1) = 1$.

Ta lại để ý thấy rằng

$$|x_1| < |x_0|.$$

Như vậy trong cả hai trường hợp chúng ta đều thấy rằng từ giả thiết về sự tồn tại một nghiệm nguyên khác không x_0, y_0, z_0 với $(x_0, y_0, z_0) = 1$ của phương trình (4) ta lại suy ra sự tồn tại một nghiệm nguyên khác không x_1, y_1, z_1 của phương trình ấy với $(x_1, y_1, z_1) =$ $= 1$ và $|x_1| < |x_0|$.

Lặp lại lí luận ở trên vô số lần với mỗi số nguyên $k = 0, k = 1, k = 2,...$ ta tìm được một nghiệm nguyên khác không x_k, y_k, z_k của phương trình (4) với $|x_{k+1}| <$ $< |x_k|$.

Điều này vô lý vì không thể tồn tại vô số số nguyên khác không $x_0, x_1, x_2,...$ thỏa mãn

$$|x_0| > |x_1| > |x_2| > ...$$

Điều vô lý này chứng tỏ rằng phương trình $x^3 + y^3 =$ $= z^3$ không có nghiệm nguyên khác không.

Tìm nghiệm nguyên của phương trình nguyên là một trong những vấn đề lớn của bộ môn số luận, đã thu hút sự quan tâm của nhiều nhà toán học. Tuy nhiên cũng phải nói rằng đây là một vấn đề hứng thú song rất khó. Về sau, chúng ta sẽ nêu lên một phương pháp để giải quyết vấn đề này, đó là phương pháp đồng dư.

BÀI TẬP

5.1. Giải các phương trình vô định sau đây :

a) $5x + 3y = 2$; b) $32x - 40y = 28$; c) $38x + 117y = 209$; d) $258x - 175y = 113$; e) $1657x - 367y = 23$.

5.2. Giải và biện luận theo số nguyên m, các phương trình vô định sau đây:

a) $6x + 11y = m + 2$; b) $15x + 25y = 2m - 1$; c) $3x - (m - 2)y = m + 1$; d) $3x + (2m-1)y = m + 1$; d) $5x + (3m + 1)y = 2m + 1$.

5.3. Giải phương trình nguyên $ax + by = c$ với $a^n + b^n = c$ và $(a, b, c) = 1$.

5.4. Với những giá trị nguyên nào của x ta có $\frac{5x + 2}{17}$ là một số nguyên?

5.5. Chứng minh rằng với mỗi cặp số nguyên dương, m, n có một phương trình bậc nhất hai ẩn $ax + by = c$ với hệ số a, b, c là những số nguyên, nhận $x = m$, $y = n$ là nghiệm nguyên dương duy nhất.

5.6. Chứng minh rằng với mỗi số nguyên dương m cho trước bao giờ cũng có một phương trình nguyên bậc nhất hai ẩn $ax + by = c$ có đúng m nghiệm nguyên dương.

5.7. Giải các phương trình vô định:

a) $2x + 3y + 5z = 15$; b) $23x - 53y + 80z = 101$; c) $56x + 92y = 12 + 17z$; d) $105x - 385y + 77z - 429t = 12$.

5.8. Giải các hệ phương trình vô định sau đây:

a) $\begin{cases} 3x + 2y = 1; \\ 3x + 6y + 2z = -1; \end{cases}$ b) $\begin{cases} 2x - 3y = 1; \\ 3x - 2y + 3z = 5; \end{cases}$

c) $\begin{cases} x + 4y + 2z = 7, \\ 2x - 7y - 5z = -7; \end{cases}$ d) $\begin{cases} 3x - 5y - 3z = 1; \\ 2x - 3y + 3z = -3; \end{cases}$

d) $\begin{cases} 2x + 3y - 5z = 2; \\ 3x - 5y + 2z = 3. \end{cases}$

5.9. Giải và biện luận theo số nguyên m, các hệ phương trình vô định sau đây:

a) $\begin{cases} 3x + 2y = 1, \\ 3x + 6y + (m + 1)z = m - 2. \end{cases}$ b) $\begin{cases} 2x - 3y = 1, \\ 3x - 2y + (2m + 1)z = 4m + 1 \end{cases}$

c) $\begin{cases} 2x - 3y = 1, \\ 3x - 2y + (2m + 1)z = 4m + 5 \end{cases}$ d) $\begin{cases} 3x - 5y - 3z = 1 \\ 2x - 3y + (m - 2)z = 1 - m; \end{cases}$

e) $\begin{cases} 3x - 3y \text{ [illegible] } z = 1, \\ 2x - 3y + (m - 2)z = 5 - m. \end{cases}$

5.10. Tìm tất cả các số tự nhiên x sao cho :

a) x chia hết cho 9 và $x + 1$ chia hết cho 25 ;

b) x chia hết cho 21 và $x + 1$ chia hết cho 165 ;

c) x chia hết cho 9, $x + 1$ chia hết cho 25 và $x + 2$ chia hết cho 4

(Thi học sinh giỏi Toán miền Bắc — 1974)

5.11. Tìm các chữ số x và y sao cho nếu chia số $\overline{xxxxx}$ cho $\overline{yyyy}$ có thương là 16 và số dư là r và nếu chia $\overline{xxxx}$ cho $\overline{yyy}$ thì cũng có thương là 16 nhưng số dư nhỏ hơn r là 2000.

(Kí hiệu $\overline{a_n a_{n-1} \ldots a_1 a_0}$ là số tự nhiên ghi trong hệ thập phân, cụ thể

$$\overline{a_n a_{n-1} \ldots a_1 a_0} = a_n \cdot 10^n + a_{n-1} \cdot 10^{n-1} + \ldots + a_1 \cdot 10 + a_0,$$

trong đó $1 \leqslant a_n \leqslant 9$, $0 \leqslant a_i \leqslant 9$ $(i = 0, 1, \ldots, n-1.)$

5.12. Trong hệ ghi cơ số thập phân hãy tìm một số thỏa mãn : nếu viết số đó trong hệ cơ số năm thì nó là một số có ba chữ số, nếu viết số đó trong hệ cơ số tám thì nó là một số có ba chữ số như trên nhưng với thứ tự ngược lại.

5.13. Hãy tìm tất cả các số nguyên mà khi chia chúng cho 19 và 11 dư tương ứng là 4 và 1.

5.14. Hãy tìm các số nguyên x sao cho $\dfrac{3x-1}{7}$ và $\dfrac{7x-1}{5}$ là những số nguyên.

5.15. Hãy tìm tất cả các số dạng $\overline{xy2}$ mà nó chia hết cho 28.

5.16. Hãy tìm tất cả các số nguyên x và y sao cho cả hai số $3x - y + 1$ và $2x + 3y - 1$ cùng chia hết cho 7.

5.17. Trên đường thẳng $8x - 13y + 6 = 0$ hãy tìm các điểm nguyên nằm giữa hai đường thẳng $x = -10$, $x = 50$.

5.18. Chứng minh rằng trong hình chữ nhật giới hạn bởi các đường thẳng

$$x = 6,\ x = 42,\ y = 2,\ y = 17$$

không có điểm nguyên nào thuộc đường thẳng $3x + 5y = 7$.

5.19. Một bài toán cổ

« Mai em đi chợ phiên
Anh gửi một tiền (*)

(*) Một tiền gồm 60 đồng.

Mua cam cùng quít
Không nhiều thì ít
Mua lấy một trăm :
Cam ba đồng một.
Quýt một đồng năm.
Thanh yên tươi tốt
Năm đồng một trái ».
Hỏi mua mỗi thứ mấy trái?

5.20. Trong các số tự nhiên từ 200 đến 500 những số nào chia cho 4, 5, 7 dư lần lượt là 3, 4, 5?

5.21. Tìm số tự nhiên nhỏ nhất sao cho khi chia nó cho 7, 5, 3, 11 ta được các số dư lần lượt là 3, 2, 1, 9.

5.22. Trên trục hoành hãy tìm tất cả các điểm nguyên mà tại đó ta dựng được đường vuông góc với trục hoành cắt, cả ba đường thẳng sau đây tại các điểm nguyên : $x=2+5y$, $x=1+8y$ $x = 3 + 11y$.

5.23. Hãy tìm tất cả các điểm nguyên mà tại đó ta dựng những đường thẳng vuông góc với hai trục tọa độ cắt cả ba đường thẳng sau đây tại các điểm nguyên : $2x-3y=4$, $5x-7y=2$, $3x + 5y = 3$.

5.24. Giải các phương trình nguyên :
a) $x^2-3y^2=1$; b) $x^2-6y^2=1$; c) $x^2-13y^2=1$; d) $x^2-31y^2=1$; e) $x^2 - 41y^2 = 1$.

5.25. Giải phương trình vô định $3x^2-2y^2=1$.

5.26. Giải phương trình vô định
$$(x-1)^2 + x^2 + (x + 1)^2 = y^2 + (y + 1)^2.$$

5.27. Tìm tất cả các số nguyên dương n sao cho hai số $2n+1$ và $3n+1$ cùng là những số chính phương.

5.28. Giải phương trình nguyên $x^2 + x = 2y^2$.

5.29. Tìm các số tam giác mà bình phương của chúng lại là một số tam giác.

5.30. Chứng minh bằng sơ cấp (không sử dụng lý thuyết về phương trình Pell) rằng : nếu $A=m^2+1$ (m là số nguyên dương) thì phương trình $x^2-Ay^2=1$ có vô số nghiệm nguyên.

5.31. Giải phương trình $x^2-Ay^2=-1$ trong tập hợp các số nguyên với A là một số nguyên dương không là chính phương.

5.32. Giải phương trình nguyên $x^2-2y^2=-1$.

5.33. Giải phương trình nguyên $x^2-2y^2=2$.

5. 34. a) Chứng minh rằng với k là một số hữu tỷ, đường thẳng $y = kx - 1$ cắt đường tròn $x^2 + y^2 = 1$ tại tất cả các điểm hữu tỷ của đường tròn.

b) Áp dụng kết quả đó tìm tất cả các nghiệm nguyên dương của phương trình $x^2 + y^2 = z^2$.

5. 35. Tìm nghiệm nguyên dương của phương trình

$$x^2 + y^2 = 2z^2.$$

5. 36. Tìm nghiệm nguyên dương của phương trình

$$x^2 + 2y^2 = z^2.$$

5. 37. Chứng minh rằng phương trình $x^2 + y^2 = 3z^2$ không có nghiệm nguyên khác không.

5. 38. Tìm nghiệm nguyên dương của phương trình

$$x^2 + y^2 + z^2 = u^2.$$

5. 39. Tìm nghiệm nguyên dương của phương trình

$$x^2 + y^2 + z^2 + u^2 = t^2.$$

5. 40. Cho biết các cạnh kề với góc 60° của một tam giác có số đo là những số nguyên. Tìm hai cạnh ấy.

5. 41. Biết rằng góc của một tam giác bằng 120° và hai cạnh kề nó có số đo là những số nguyên. Hãy tìm độ dài hai cạnh ấy.

5. 42. Chứng minh rằng phương trình $x^4 + 2y^4 = z^2$ không có nghiệm nguyên khác không.

5. 43 Chứng minh rằng phương trình $x^4 + 2y^4 = z^4$ không có nghiệm nguyên khác không.

5. 44. Chứng minh rằng hai định lý sau đây tương đương với nhau :

Định lý 1 : « Phương trình $\frac{x}{y} + \frac{y}{z} = \frac{z}{x}$ không có nghiệm nguyên dương ».

Định lý 2 : « Phương trình $u^3 + v^3 = t^3$ không có nghiệm nguyên dương ».

5. 45. Chứng minh rằng với mọi số nguyên $n > 2$, phương trình : $x^n + y^n = z^n$ không có nghiệm nguyên dương x, y, z với $z < 1 + \frac{1}{\sqrt[n]{2} - 1}$

BÀI THỨ SÁU

LÝ THUYẾT ĐỒNG DƯ

§ 1. ĐỒNG DƯ THỨC

Trong bài này chúng ta sẽ nghiên cứu quan hệ giữa các số nguyên về phương diện số dư trong phép chia các số nguyên cho một số tự nhiên.

I — ĐỊNH NGHĨA ĐỒNG DƯ THỨC

1. Định nghĩa. Cho m là một số tự nhiên khác không. Ta nói hai số nguyên a và b là *đồng dư với nhau theo môđun m* nếu trong phép chia a và b cho m ta được cùng một số dư.

Khi a và b đồng dư với nhau theo môđun m ta viết

$$a \equiv b \pmod{m} \qquad (1)$$

Hệ thức (1) gọi là một *đồng dư thức.*

Ví dụ $9 \equiv 3 \pmod{6}$; $8 \not\equiv 4 \pmod{6}$; $8 \not\equiv 3 \pmod{6}$.

$3 \equiv -4 \pmod{6}$

2. Các điều kiện tương đương với định nghĩa.

Định lý. *Các mệnh đề sau đây là tương đương:*

(*a*) $a \equiv b \pmod{m}$;

(*b*) $m \mid a - b$;

(*c*) *có số nguyên t sao cho* $a = b + mt$.

Chứng minh. Ta sẽ chứng minh (a) ⇒ (b) ⇒ (c) ⇒ (a).

(a) ⇒ (b). Theo định nghĩa của $a \equiv b \pmod{m}$, ta có $a = mq_1 + r$, $b = mq_2 + r$, $q_1, q_2, r \in \mathbb{Z}$, $0 \leqslant r < m$. Từ đó ta được $a - b = m(q_1 - q_2)$ tức là $m \mid a - b$.

(b) ⇒ (c). Giả sử $m \mid a - b$, khi ấy ắt có $t \in \mathbb{Z}$ sao cho $a - b = mt$, nghĩa là $a = b + mt$, $t \in \mathbb{Z}$.

(c) ⇒ (a). Giả sử có số nguyên t sao cho $a = b + mt$. Gọi r là số dư trong phép chia a cho m, nghĩa là

$$a = mq_1 + r,\ q_1,\ r \in Z,\ 0 \leqslant r < m.$$

Khi ấy ta có

$$b + mt = mq_1 + r$$

hay là

$$b = m(q_1 - t) + r,$$

trong đó $q_1 - t$ là một số nguyên và $0 \leqslant r < m$, cho nên số dư trong phép chia b cho m cũng là r, nói khác đi $a \equiv b \pmod m$.

Định lý được chứng minh.

Định lý này cho phép ta lấy mệnh đề (b) hoặc mệnh đề (c) trong định lý thay cho định nghĩa khái niệm đồng dư. Trong thực tế người ta hay dùng các mệnh đề (b) hoặc (c) hơn, bởi vì các mệnh đề này đưa khái niệm đồng dư về các khái niệm đã quen biết là chia hết và bằng nhau có thể diễn tả bởi các đẳng thức.

Chúng ta chú ý rằng, trường hợp đặc biệt $a \equiv 0 \pmod m$ có nghĩa là a chia hết cho m.

II – CÁC TÍNH CHẤT CỦA ĐỒNG DƯ THỨC

1. ***Quan hệ đồng dư là một quan hệ tương đương trên tập hợp số nguyên*, nghĩa là nó có các tính chất đơn giản sau đây:**

a) với mọi số nguyên a ta có $a \equiv a \pmod m$;

b) nếu $a \equiv b \pmod m$ thì $b \equiv a \pmod m$;

c) nếu $a \equiv b \pmod m$ và $b \equiv c \pmod m$ thì $a \equiv c \pmod m$.

Chứng minh. a) Với số nguyên a tùy ý ta có

$$a - a = 0 \vdots m \text{ nên } a \equiv a \pmod m.$$

b) Từ $a \equiv b \pmod{m}$ ta có $m \mid a - b$, khi ấy cũng có $m \mid b - a$ cho nên $b \equiv a \pmod{m}$.

c) Từ $a \equiv b \pmod{m}$ và $b \equiv c \pmod{m}$ ta có $m \mid a - b$ và $m \mid b - c$, khi ấy $m \mid (a - b) + (b - c)$ hay $m \mid a - c$, nghĩa là $a \equiv c \pmod{m}$.

2. a) *Ta có thể cộng hoặc trừ từng vế một của nhiều đồng dư thức theo cùng một môđun.* Cụ thể là nếu có $a_i \equiv b_i \pmod{m}$, $i = 1, 2, \ldots, k$ thì ta cũng có

$$a_1 \pm a_2 \pm \ldots \pm a_k \equiv b_1 \pm b_2 \pm \ldots \pm b_k \pmod{m}.$$

b) *Ta có thể nhân từng vế một với nhau nhiều đồng dư thức theo cùng một môđun.* Cụ thể là nếu có $a_i \equiv b_i \pmod{m}$, $i = 1, 2, \ldots, k$ thì ta cũng có $a_1a_2\ldots a_k \equiv b_1b_2\ldots b_k \pmod{m}$.

Chứng minh. Từ $a_i \equiv b_i \pmod{m}$, $i = 1, 2, \ldots, k$ suy ra ắt có $t_i \in \mathbf{Z}$, $i = 1, 2, \ldots, k$ sao cho

$$a_i = b_i + mt_i, \quad i = 1, 2, \ldots, k. \qquad (2)$$

Cộng (hoặc trừ) từng vế một các đẳng thức (2) ta sẽ được

$$a_1 \pm a_2 \pm \ldots \pm a_k = b_1 \pm b_2 \pm \ldots \pm b_k + m(t_1 \pm t_2 \pm \ldots \pm t_k).$$

Đẳng thức này chứng tỏ

$$a_1 \pm a_2 \pm \ldots \pm a_k \equiv b_1 \pm b_2 \pm \ldots \pm b_k \pmod{m}.$$

Ta lại nhân từng vế một các đẳng thức (2) ta sẽ được một đẳng thức mà ở vế phải, ngoài số hạng là tích $b_1b_2\ldots b_k$ còn các số hạng khác đều có ít nhất một thừa số m nên ta có

$$a_1a_2\ldots a_k = b_1b_2\ldots b_k + mt, \quad t \in \mathbf{Z}.$$

Đẳng thức này chứng tỏ

$$a_1a_2\ldots a_k \equiv b_1b_2\ldots b_k \pmod{m}.$$

3. *Các hệ quả của tính chất 2.*

a) *Ta có thể thêm vào hay bớt đi cùng một số vào hai vế của một đồng dư thức,* nghĩa là nếu ta có

$$a \equiv b \pmod{m}$$

thì ta cũng có

$$a \pm c \equiv b \pm c \pmod{m}$$

với c là một số nguyên tùy ý.

Chứng minh. Thật vậy, theo giả thiết $a \equiv b \pmod{m}$ và theo tính chất 1 $c \equiv c \pmod{m}$ nên áp dụng tính chất 2 ta được $a \pm c \equiv b \pm c \pmod{m}$.

b) *Ta có thể chuyển vế các số hạng của một đồng dư thức nhưng phải đổi dấu của số hạng đó*, nghĩa là nếu có

$$a + c \equiv b \pmod{m}$$

thì ta cũng có

$$a \equiv b - c \pmod{m}.$$

Chứng minh. Từ đồng dư thức $a + c \equiv b \pmod{m}$, áp dụng hệ quả trên bằng cách cộng vào hai vế của nó với cùng một số $(-c)$ ta sẽ được $a \equiv b - c \pmod{m}$.

c) *Ta có thể thêm vào hay bớt đi ở một vế của một đồng dư thức một bội của môđun*, nghĩa là nếu ta có

$a \equiv b \pmod{m}$ thì ta cũng có

$$a + km \equiv b \pmod{m} \text{ với mọi } k \in \mathbf{Z}.$$

Chứng minh. Thật vậy ta có $a \equiv b \pmod{m}$ và $km \equiv 0 \pmod{m}$ nên áp dụng tính chất 2 ta được

$$a + km \equiv b \pmod{m}$$

d) *Ta có thể nhân hai vế của một đồng dư thức với cùng một số nguyên tùy ý*, nghĩa là nếu ta có

$$a \equiv b \pmod{m}$$

thì ta cũng có

$$ac \equiv bc \pmod{m} \text{ với mọi } c \in \mathbf{Z}.$$

Chứng minh. Thật vậy ta có $a \equiv b \pmod{m}$ và $c \equiv c \pmod{m}$ nên áp dụng tính chất 2 ta được $ac \equiv bc \pmod{m}$.

e) *Ta có thể nâng lên lũy thừa bậc nguyên dương tùy ý hai vế của một đồng dư thức*, nghĩa là nếu có

$$a \equiv b \pmod{m}$$

thì ta cũng có

$$a^n \equiv b^n \pmod{m}$$

với n là một số nguyên dương.

Chứng minh. Áp dụng tính chất 2 bằng cách nhân đồng dư thức $a \equiv b \pmod{m}$ với chính nó từng vế một n lần, chúng ta được kết quả cần chứng minh.

g) *Giả sử* $f(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0$ *là một đa thức với hệ số nguyên. Nếu ta có*

$$\alpha \equiv \beta \pmod{m}.$$

thì ta cũng có

$$f(\alpha) \equiv f(\beta) \pmod{m}$$

Đặc biệt nếu ta có

$$f(\alpha) \equiv 0 \pmod{m}$$

thì ta cũng có

$$f(\alpha + km) \equiv 0 \pmod{m} \text{ với mọi } k \in \mathbf{Z}.$$

Chứng minh. Theo giả thiết $\alpha \equiv \beta \pmod{m}$ do đó

$$a_i\alpha^i \equiv a_i\beta^i \pmod{m} \text{ với } i = 1, 2, \ldots, n.$$

Từ đó ta được

$$a_n\alpha^n + a_{n-1}\alpha^{n-1} + \ldots + a_1\alpha + a_0 \equiv a_n\beta^n + a_{n-1}\beta^{n-1} + \ldots +$$
$$+ a_1\beta + a_0 \pmod{m},$$

nghĩa là

$$f(\alpha) \equiv f(\beta) \pmod{m}.$$

Đặc biệt vì $\alpha \equiv \alpha + km \pmod{m}$, $k \in \mathbf{Z}$, nên $f(\alpha) \equiv f(\alpha + km) \pmod{m}$. Nhưng $f(\alpha) \equiv 0 \pmod{m}$ nên ta cũng có $f(\alpha + km) \equiv 0 \pmod{m}$.

4. *Ta có thể chia hai vế của một đồng dư thức cho một ước chung của hai vế, nguyên tố với môđun.* Cụ thể là nếu ta có

$$ac \equiv bc \pmod{m} \text{ và } (c, m) = 1$$

thì ta cũng có

$$a \equiv b \pmod{m}.$$

Chứng minh. Theo giả thiết $ac \equiv bc \pmod{m}$ vậy $m \mid ac - bc$ hay $m \mid c(a-b)$. Nhưng $(c,m) = 1$ nên ta phải có $m \mid a-b$, nghĩa là $a \equiv b \pmod{m}$.

5. a) *Ta có thể nhân hai vế và môđun của một đồng dư thức với cùng một số nguyên dương.* Cụ thể là nếu ta có
$$a \equiv b \pmod{m}$$
thì cũng có
$$ac \equiv bc \pmod{mc}$$
với c là một số nguyên dương.

b) *Ta có thể chia hai vế và môđun của một đồng dư thức cho một ước chung dương của chúng.* Cụ thể là nếu ta có $a \equiv b \pmod{m}$ và $\delta > 0$, $\delta \mid (a, b, m)$ thì ta cũng có

$$\frac{a}{\delta} \equiv \frac{b}{\delta} \left(\bmod \frac{m}{\delta}\right).$$

Chứng minh. a) Theo giả thiết $a \equiv b \pmod{m}$ vậy có số nguyên t sao cho $a = b + mt$. Nhân hai vế của đẳng thức này với c ta được $ac = bc + mct$, nghĩa là $ac \equiv bc \pmod{mc}$.

b) Từ giả thiết $\delta \mid (a, b, m)$ ta đặt $a = \delta a_1$, $b = \delta b_1$, $m = \delta m_1$ với $a_1, b_1, m_1 \in Z$. Nhưng $a = b + mt$ nên $\delta a_1 = \delta b_1 + \delta m_1 t$. Chia cả hai vế cho δ ta được $a_1 = b_1 + m_1 t$, nghĩa là

$a_1 \equiv b_1 \pmod{m_1}$ hay là $\dfrac{a}{\delta} \equiv \dfrac{b}{\delta} \left(\bmod \dfrac{m}{\delta}\right)$.

6. *Nếu hai số a và b đồng dư với nhau theo nhiều môđun thì chúng cũng đồng dư với nhau theo môđun là BCNN của các môđun đó.* Cụ thể là nếu ta có
$$a \equiv b \pmod{m_i},\ i = 1, 2, \ldots, k$$
thì ta cũng có
$$a \equiv b \pmod{m},$$
trong đó $m = [m_1, m_2, \ldots, m_k]$.

Chứng minh. Thật vậy theo giả thiết, $a-b$ là bội chung của $m_1, m_2, \ldots, m_k$ nên $a-b$ cũng là bội của $m=[m_1, m_2, \ldots, m_k]$ nghĩa là $a \equiv b \pmod{m}$.

7. *Nếu a và b đồng dư với nhau theo môđun m thì chúng cũng đồng dư với nhau theo môđun là ước của m.* Cụ thể là nếu $a \equiv b \pmod{m}$ và $\delta \mid m$, $\delta > 0$, thì ta cũng có

$$a \equiv b \pmod{\delta}.$$

Chứng minh. Theo giả thiết $m \mid a-b$ mà $\delta \mid m$ nên $\delta \mid a-b$ nghĩa là $a \equiv b \pmod{\delta}$.

8. *Nếu a và b đồng dư với nhau theo môđun m thì tập hợp các ước chung của a và m trùng với tập hợp các ước chung của b và m. Đặc biệt ta có $(a, m)=(b, m)$.*

Thật vậy, bởi vì $a \equiv b \pmod{m}$ nên ắt có $t \in Z$ sao cho $a=b+mt$. Đẳng thức này chứng tỏ rằng tập hợp các ước chung của a và m trùng với tập hợp các ước chung của b và m, và do đó ta có $(a, m)=(b, m)$.

§ 2. CÁC LỚP THẶNG DƯ

1 – HỆ THẶNG DƯ ĐẦY ĐỦ

1. Định nghĩa. Cho m là một số tự nhiên lớn hơn 1, khi ấy tập hợp $H=\{0, 1, \ldots, m-1\}$ gồm các số nguyên đôi một không đồng dư với nhau theo môđun m và mọi số nguyên đều đồng dư với một số nào đó của H.

Thật vậy với $a, b \in H$, $a \neq b$ ta có $0 < |a-b| < m$ nên $a \not\equiv b \pmod{m}$.

Giả sử x là một số nguyên tùy ý, thế thì ắt có cặp số nguyên q, r sao cho $x=qm+r$, $0 \leqslant r < m$. Các hệ thức này chứng tỏ $x \equiv r \pmod{m}$, $r \in H$.

Hệ các số nguyên $H=\{0, 1, \ldots, m-1\}$ được gọi là *hệ thặng dư đầy đủ môđun m không âm nhỏ nhất.*

Tổng quát ta có định nghĩa: *một tập hợp H những số nguyên được gọi là một hệ thặng dư đầy đủ theo môđun m* (viết tắt là hệ TDĐĐ modm) nếu và chỉ nếu:

— các số nguyên trong H đôi một không đồng dư với nhau theo môđun m;

— mọi số nguyên đều đồng dư theo môđun m với một số nào đó trong H.

Mỗi một số nguyên của H được gọi là một *thặng dư*.

2. Ví dụ.

a) Với m = 6 ta có {0, 1, 2, 3, 4, 5} là hệ thặng dư đầy đủ không âm nhỏ nhất: {−2, −1, 0, 1, 2, 3} là một hệ thặng dư đầy đủ giá trị tuyệt đối nhỏ nhất.

b) Hệ thặng dư đầy đủ môđun m sau đây được gọi là hệ *thặng dư đầy đủ giá trị tuyệt đối nhỏ nhất*:

$$H = \left\{-\frac{m-1}{2}, -\frac{m-1}{2}+1, \ldots, \frac{m-1}{2}\right\}$$ nếu m là số lẻ;

$$H = \left\{-\frac{m}{2}, -\frac{m}{2}+1, \ldots, \frac{m}{2}-1\right\}$$ hoặc là

$$H = \left\{-\frac{m}{2}+1, -\frac{m}{2}+2, \ldots, \frac{m}{2}\right\}$$ nếu m là số chẵn.

3. Tính chất

a) *Mỗi hệ thặng dư đầy đủ môđun m đều gồm m thặng dư.*

Chứng minh: Giả sử H là một hệ TDĐĐ modm, thế thì H gồm có đúng m số. Thật vậy, nếu H có nhiều hơn m số thì trong H sẽ có ít nhất hai số có hiệu chia hết cho m (bài tập 3a) bài thứ nhất), nghĩa là trong H có hai số đồng dư với nhau theo môđun m là điều không thể được. Nếu H có ít hơn m phần tử thì trong hệ {0, 1, 2, ..., m−1} sẽ có hai số cùng đồng dư với một số

nào đó trong H, từ đó suy ra rằng trong hệ $\{0, 1, 2, ..., m-1\}$ có hai số nào đó đồng dư với nhau theo môđun m cũng là điều không thể được. Vậy H có đúng m thặng dư.

b) *Mọi hệ gồm m số nguyên đôi một không đồng dư với nhau theo môđun m đều hợp thành một hệ thặng dư đầy đủ môđun m.*

Chứng minh. Giả sử $H = \{a_0, a_1, ..., a_{m-1}\}$ là hệ gồm m số nguyên đôi một không đồng dư với nhau theo môđun m. Ta phải chứng minh rằng mỗi số nguyên x đều đồng dư với một số nào đó thuộc H.

Bằng cách chia $a_0, a_1, ..., a_{m-1}$ cho m ta được
$a_i = mq_i + r_i$, $q_i, r_i \in Z$, $0 \leqslant r_i < m$, $i = 0, 1, ..., m-1$.

Dễ thấy rằng tập hợp $\{r_i \mid i = 0, 1, ..., m-1\}$ là tập hợp $\{0, 1, ..., m-1\}$. Thật vậy với $i \neq j$, $0 \leqslant i, j \leqslant m-1$ thì $r_i \neq r_j$, bởi vì nếu $r_i = r_j$ thì ta có $a_i \equiv a_j \pmod{m}$, $i \neq j$, trái với giả thiết là các phần tử của H đôi một không đồng dư với nhau theo môđun m.

Giả sử x là một số nguyên tùy ý, chia x cho m ta được

$$x = mq + r,\ q,\ r \in Z,\ 0 \leqslant r < m.$$

Từ đó r phải là một số r_i nào đó với $i = 0, 1, ..., m-1$ và $x \equiv r \pmod{m}$. Bởi vậy $x \equiv r_i \pmod{m}$ và vì $a_i \equiv r_i \pmod{m}$ nên $x \equiv a_i \pmod{m}$ với i nào đó $(0 \leqslant i \leqslant m-1)$.

c) *Cho a là một số nguyên nguyên tố với m và b là một số nguyên tùy ý. Khi ấy nếu x chạy qua một hệ thặng dư đầy đủ môđun m thì ax + b cũng chạy qua một hệ thặng dư đầy đủ môđun m.*

Chứng minh Giả sử x chạy qua một hệ thặng dư đầy đủ môđun m $\{x_1, x_2, ..., x_m\}$ ta phải chứng minh $\{ax_1 + b, ax_2 + b, ..., ax_m + b\}$ cũng là một hệ thặng dư đầy đủ môđun m. Theo tính chất b) ở trên ta chỉ cần chứng

minh rằng với $i \neq j$ $(1 \leqslant i, j \leqslant m)$ có $ax_i + b \not\equiv ax_j + b$ (modm). Thật vậy nếu như $ax_i + b \equiv ax_j + b$ (modm), thì

$$ax_i \equiv ax_j \pmod{m}$$

từ đó do $(a, m) = 1$ ta có

$$x_i \equiv x_j \pmod{m}, \ i \neq j.$$

Điều này là không thể được vì x_i và x_j là hai thặng dư khác nhau của một hệ TDĐĐ modm.

II — CÁC LỚP THẶNG DƯ

1. Giả sử $H = \{a_0, a_1, ..., a_{m-1}\}$ là một hệ TDĐĐ modm. Ta xét bộ phận $\overline{a_i}$ $(i = 0, 1, ..., m-1)$ của tập hợp số nguyên **Z** xác định như sau:

$\overline{a_i} = \{x \in \mathbf{Z} \mid x \equiv a_i \pmod{m}\}$, $(i = 0, 1, ..., m-1)$.

Ta gọi $\overline{a_0}, \overline{a_1}, ..., \overline{a_{m-1}}$ xác định như thế là những *lớp thặng dư theo môđun m.*

2. *Giả sử $H = \{a_0, a_1, ..., a_{m-1}\}$ là một hệ TDĐĐ modm. Khi ấy ta có:*

a) $\bigcup_{i=0}^{m-1} \overline{a_i} = \mathbf{Z}$;

b) $\overline{a_i} \cap \overline{a_j} = \phi$, $i \neq j$ $(0 \leqslant i, j \leqslant m-1)$.

Chứng minh:

a) Rõ ràng $\bigcup_{i=0}^{m-1} \overline{a_i} \subset \mathbf{Z}$. Ngược lại ta có $\mathbf{Z} \subset \bigcup_{i=0}^{m-1} \overline{a_i}$, thật vậy giả sử $x \in \mathbf{Z}$, khi ấy ắt có a_i $(0 \leqslant i \leqslant m-1)$ để $x \equiv a_i$ (modm), nói khác đi $x \in \overline{a_i}$.

Điều này kéo theo $x \in \bigcup_{i=0}^{m-1} \overline{a_i}$.

b) Ta chứng minh với $i \neq j$ $(0 \leqslant i, j \leqslant m-1)$ thì $\overline{a_i} \cap \overline{a_j} = \phi$. Thật vậy nếu $\overline{a_i} \cap \overline{a_j} \neq \phi$ thì ắt có $x \in \overline{a_i}$ và $x \in \overline{a_j}$, từ đó suy ra $x \equiv a_i$ (modm) và $x \equiv a_j$ (modm), và từ đó ta có $a_i \equiv a_j$ (modm). Điều này là không thể được vì a_i, a_j là hai thặng dư khác nhau của một hệ TDĐĐ modm.

3. *Tập hợp các lớp thặng dư đầy đủ môđun m, ký hiệu bởi Z_m, có m phần tử.* Gọi các phần tử của Z_m là $A_0, A_1, \ldots, A_{m-1}$ ta sẽ có

$Z_m = \{A_0, A_1, \ldots, A_{m-1}\} = \{\overline{a_0}, \overline{a_1}, \ldots, \overline{a_{m-1}}\} = \{\overline{0}, \overline{1}, \ldots, \overline{m-1}\}$.

Ta có thể định nghĩa một hệ TDĐĐ modm là một tập hợp gồm các số nguyên lấy ở mỗi lớp thặng dư môđun m một và chỉ một số.

4. *Tất cả các thặng dư của cùng một lớp thặng dư có cùng các ước chung với môđun, nói riêng có cùng ước chung lớn nhất với môđun.*

Thật vậy, điều này suy ra trực tiếp từ tính chất 8, II, § 1.

Ước chung lớn nhất của các thặng dư của cùng một lớp thặng dư với môđun được gọi là *ước chung lớn nhất của lớp đó với môđun*, hay trong những lúc không sợ lầm lẫn ta gọi là *ước chung lớn nhất của lớp đó.*

Cụ thể là nếu $d = (a, m)$ với $a \in A$ thì ta đặt $(A, m) = d$.

Nếu ước chung lớn nhất của một lớp với môđun mà bằng 1 thì ta nói *lớp đó nguyên tố với môđun*, hay không sợ lầm lẫn gọi tắt là *lớp nguyên tố.*

III – HỆ THẶNG DƯ THU GỌN

1. Các lớp thặng dư thu gọn. Cho Z_m là tập hợp các lớp thặng dư môđun m. Bộ phận Z_m^* gồm các lớp của

$\mathbb{Z}_m$, nguyên tố với môđun, được gọi là *tập hợp các lớp thặng dư thu gọn môđun m*.

$$\mathbb{Z}_m^* = \{ A \in \mathbb{Z}_m \mid (A, m) = 1 \}.$$

Hệ quả. *Tập hợp* $\mathbb{Z}_m^*$ *có đúng* $\varphi(m)$ *phần tử.*

Thật vậy, ta có $\mathbb{Z}_m = \{\overline{0}, \overline{1}, ..., \overline{m-1}\}$ cho nên

$$\mathbb{Z}_m^* = \{\overline{a} \in \mathbb{Z}_m \mid (a, m) = 1,\ 0 \leqslant a \leqslant m-1\}$$

mà trong tập hợp $\{0, 1, ..., m-1\}$ có $\varphi(m)$ số nguyên tố với m. Vậy $\mathbb{Z}_m^*$ có $\varphi(m)$ phần tử.

2. Hệ thặng dư thu gọn. Trong mỗi lớp của $\mathbb{Z}_m^*$ ta lấy ra một và chỉ một thặng dư thì ta có một tập hợp những số nguyên được gọi là một *hệ thặng dư thu gọn theo môđun m* (viết tắt là hệ TDTG modm).

Vậy một tập hợp K gồm những số nguyên được gọi là *một hệ thặng dư thu gọn môđun m* nếu và chỉ nếu :

— đôi một các phần tử thuộc K không đồng dư với nhau theo môđun m ;

— các số trong K đều nguyên tố với môđun m ;

— mỗi số nguyên tùy ý nguyên tố với môđun m đều đồng dư với một số nào đó thuộc K.

Người ta cũng nói đến *hệ TDTG môđun m không âm nhỏ nhất* và hệ *TDTG modm giá trị tuyệt đối nhỏ nhất*.

Ví dụ. m = 6 ta có $\{1, 5\}$ là hệ TDTG không âm nhỏ nhất ; $\{-1, 1\}$ là hệ TDTG giá trị tuyệt đối nhỏ nhất.

Nếu m = p là số nguyên tố thì $\{1, 2, ..., p-1\}$ là hệ thặng dư thu gọn không âm nhỏ nhất và thêm nữa $p > 2$ thì $\left\{-\frac{p-1}{2}, ..., -2, -1, 1, 2, ..., \frac{p-1}{2}\right\}$ là hệ thặng dư thu gọn giá trị tuyệt đối nhỏ nhất.

3. Tính chất của hệ thặng dư thu gọn.

a) Mỗi hệ thặng dư thu gọn môđun m đều gồm $\varphi(m)$ thặng dư.

Thật vậy, điều này suy ra từ hệ quả ở trên là tập hợp Z_m^* có đúng $\varphi(m)$ phần tử.

b) Mọi hệ gồm $\varphi(m)$ số nguyên nguyên tố với m và đôi một không đồng dư với nhau theo môđun m lập nên một hệ thặng dư thu gọn môđun m.

Chứng minh. Giả sử $K = \{g_1, g_2, \ldots, g_{\varphi(m)}\}$, $(g_i, m) = 1$, $g_i \not\equiv g_j \pmod m$, $i \neq j$, $1 \leqslant i, j \leqslant \varphi(m)$.

Để chứng minh K là một hệ TDTG modm ta còn phải chứng minh mỗi số nguyên nguyên tố với m đều đồng dư với một số nào đó thuộc K.

Bằng cách chia $g_1, g_2, \ldots, g_{\varphi(m)}$ cho m ta được
$g_i = mq_i + r_i$, $q_i, r_i \in Z$, $0 \leqslant r_i < m$, $(i = 1, 2, \ldots, \varphi(m))$.

Dễ thấy rằng tập hợp $\{r_i \mid i = 1, 2, \ldots, \varphi(m)\}$ là tập hợp $\{x \in Z \mid 0 \leqslant x < m, (x, m) = 1\}$. Thật vậy, với $i = 1, 2, \ldots, \varphi(m)$, ta có $(r_i, m) = (g_i, m) = 1$; mặt khác $r_i \neq r_j$ với $i \neq j$ $(1 \leqslant i, j \leqslant \varphi(m))$ bởi vì $g_i \not\equiv g_j \pmod m$ và $0 \leqslant r_i, r_j < m$.

Giả sử x là một số nguyên tùy ý nguyên tố với m và $x = mq + r$, $q, r \in Z$, $0 \leqslant r < m$. Từ đây ta có $x \equiv r \pmod m$ và $(r, m) = (x, m) = 1$. Nhưng $0 \leqslant r < m$ nên r phải là một số r_i nào đó với $i = 1, 2, \ldots, \varphi(m)$, nghĩa là $x \equiv r_i \pmod m$. Từ $x \equiv r_i \pmod m$ và $g_i \equiv r_i \pmod m$ ta suy ra $x \equiv g_i \pmod m$ với i nào đó mà $1 \leqslant i \leqslant \varphi(m)$.

c) Cho a là một số nguyên nguyên tố với m. Khi ấy nếu x chạy qua một hệ TDTG modm thì ax cũng chạy qua một hệ TDTG modm.

Chứng minh. Giả sử x chạy qua hệ TDTG modm $\{x_1, x_2, \ldots, x_{\varphi(m)}\}$, khi ấy $\{ax_1, ax_2, \ldots, ax_{\varphi(m)}\}$ cũng là một hệ TDTG modm. Thật vậy, đây là một hệ gồm

$\varphi(m)$ số nguyên nguyên tố với m bởi vì $(a, m) = 1$ và $(x_i, m) = 1$ $(i = 1, 2, \ldots, \varphi(m))$. Hơn nữa với $i \neq j$ $(1 \leqslant i, j \leqslant \varphi(m)$ ta có $ax_i \not\equiv ax_j \pmod{m}$, bởi vì nếu $ax_i \equiv ax_j \pmod{m}$ thì do $(a, m) = 1$ ta có $x_i \equiv x_j \pmod{m}$, điều này mâu thuẫn với việc x_i xà x_j là hai thặng dư khác nhau trong một hệ thặng dư thu gọn môđun m.

§ 3. ĐỊNH LÝ ƠLE VÀ ĐỊNH LÝ PHÉCMA

Trong tiết này chúng ta chứng minh hai định lý quan trọng bằng công cụ đồng dư thức.

I — ĐỊNH LÝ ƠLE

Định lý. *Cho m là một số tự nhiên khác 0 và a là một số nguyên nguyên tố với m. Khi ấy ta có*

$$a^{\varphi(m)} \equiv 1 \pmod{m}.$$

Chứng minh. Ta cho x chạy qua hệ TDTG modm không âm nhỏ nhất $\{r_1, r_2, \ldots, r_{\varphi(m)}\}$. Khi đó tập hợp $\{ar_1, ar_2, \ldots, ar_{\varphi(m)}\}$ là một hệ TDTG modm. Gọi $s_1, s_2, \ldots, s_{\varphi(m)}$ là các thặng dư không âm nhỏ nhất tương ứng cùng lớp với $ar_1, ar_2, \ldots, ar_{\varphi(m)}$ thì ta có

$$ar_1 \equiv s_1 \pmod{m},$$
$$ar_2 \equiv s_2 \pmod{m},$$
$$\ldots\ldots\ldots\ldots$$
$$ar_{\varphi(m)} \equiv s_{\varphi(m)} \pmod{m}.$$

Bằng cách nhân từng vế của $\varphi(m)$ đồng dư thức này ta được

$$a^{\varphi(m)} . r_1 r_2 \ldots r_{\varphi(m)} \equiv s_1 s_2 \ldots s_{\varphi(m)} \pmod{m}.$$

Bởi vì $r_1, r_2, \ldots, r_{\varphi(m)}$ và $s_1, s_2, \ldots, s_{\varphi(m)}$ cùng là hệ TDTG không âm nhỏ nhất nên ta có

$$r_1r_2 \dots r_{\varphi(m)} = s_1s_2 \dots s_{\varphi(m)}$$

từ đó

$$a^{\varphi(m)} r_1r_2 \dots r_{\varphi(m)} \equiv r_1r_2 \dots r_{\varphi(m)} (\text{mod} m);$$

Nhưng tích $r_1r_2 \dots r_{\varphi(m)}$ nguyên tố với m vì từng thừa số của nó nguyên tố với m, bởi vậy ta có thể chia hai vế của đồng dư thức trên đây cho $r_1 r_2 \dots r_{\varphi(m)}$ ta được

$$a^{\varphi(m)} \equiv 1 \ (\text{mod} m).$$

II – ĐỊNH LÝ PHÉCMA

1. Định lý 1. *Cho p là một số nguyên tố và a là một số nguyên không chia hết cho p. Khi ấy ta có*

$$a^{p-1} \equiv 1 \ (\text{mod} p).$$

Chứng minh. Áp dụng định lý Ơle cho trường hợp $m = p$ là một số nguyên tố thì $\varphi(p) = p - 1$ và điều kiện a không chia hết cho p có nghĩa là $(a,p) = 1$, ta được định lý Phécma.

2. Dạng khác của định lý Phécma

Định lý 2. *Cho p là một số nguyên tố và a là một số nguyên tùy ý. Khi ấy ta có*

$$a^p \equiv a \ (\text{mod} p).$$

Chứng minh. Nếu $p \mid a$ thì hiển nhiên $a^p \equiv a$ (modp), còn nếu p không chia hết a thì theo định lý 1 ta có $a^{p-1} \equiv 1$ (modp) và sau khi nhân hai vế của đồng dư thức này với a ta được $a^p \equiv a$(modp). Vậy từ định lý 1 ta suy ra được định lý 2. Ngược lại dễ dàng từ định lý 2 ta suy ra ngay được định lý 1 (4.II, §1).

III – CÁC VÍ DỤ ÁP DỤNG

Định lý Ơle và định lý Phécma có nhiều ứng dụng. ở đây ta nêu lên một vài ví dụ về việc tìm số dư trong phép chia một lũy thừa cho một số đã cho.

Ví dụ 1: Tìm số dư trong phép chia 3^{100} cho 13.

Theo định lý Phécma do 13 không chia hết 3 và $\varphi(13) = 12$ ta có

$$3^{12} \equiv 1 \pmod{13}$$

Hơn nữa $100 = 12.8 + 4$ cho nên

$$3^{100} = (3^{12})^8 . 3^4 \equiv 3^4 \pmod{13}.$$

Nhưng $3^4 = 81 \equiv 3 \pmod{13}$ nên ta có

$$3^{100} \equiv 3 \pmod{13},$$

nghĩa là dư trong phép chia 3^{100} cho 13 là 3.

Ví dụ 2. Tìm số dư trong phép chia 109^{345} cho 14

Bởi vì $109 \equiv -3 \pmod{14}$ nên $109^{345} \equiv (-3)^{345} \pmod{14}$

Theo định lý Ơle từ $(-3, 14) = 1$ ta có

$$(-3)^{\varphi(14)} \equiv 1 \pmod{14}$$

nhưng $\varphi(14) = 6$ nên

$$(-3)^6 \equiv 1 \pmod{14}.$$

Hơn nữa $345 = 6.57 + 3$ cho nên

$$(-3)^{345} = [(-3)^6]^{57} (-3)^3 \equiv -27 \pmod{14},$$

và từ $-27 \equiv 1 \pmod{14}$

ta được $109^{315} \equiv 1 \pmod{14}$, nghĩa là số dư trong phép chia 109^{345} cho 14 là 1.

Ví dụ 3. Tìm số dư trong phép chia 2^{153} cho 100. Ta thấy rằng $(2,100) = 2$ và $100 = 2^2 5^2$, bởi vậy trước hết ta hãy tìm số dư trong phép chia 2^{151} cho 25.

Từ $(2, 25) = 1$, theo định lý Ơle ta có

$2^{\varphi(25)} \equiv 1 \pmod{25}$ hay là $2^{20} \equiv 1 \pmod{25}$ bởi vì $\varphi(25) = 20$.

Mặt khác $151 \equiv 11 \pmod{20}$
nên $2^{151} \equiv 2^{11} \pmod{25}$ và do $2^{11} = 2048 \equiv -2 \pmod{25}$ ta có

$$2^{151} \equiv -2 \pmod{25}.$$

Từ đồng dư thức sau cùng ở trên sau khi nhân hai vế và môđun của đồng dư thức với 4 ta được

$$2^{153} \equiv -8 \pmod{100},$$

hay là

$$2^{153} \equiv 92 \pmod{100},$$

nói khác đi, số dư trong phép chia 2^{153} cho 100 là 92.

Ta cũng có thể nói rằng khi viết số 2^{153} trong hệ thập phân thì hai chữ số tận cùng bên phải là 92.

BÀI TẬP

6.1. Chứng minh rằng

a) $100a + 10b + c \equiv 0 \pmod{21}$ khi và chỉ khi $a - 2b + 4c \equiv 0 \pmod{21}$;

b) $3^n \equiv -1 \pmod{10}$ khi và chỉ khi $3^{n+4} \equiv -1 \pmod{10}$

6.2. Tìm số dư trong các phép chia

a) $8!$ chia cho 11 ; b) $1532^5 - 1$ chia cho 9 ; c) $(12371^{56} + 34)^{28}$ chia cho 111.

6.3. Chứng minh rằng

a) $220^{119^{69}} + 119^{69^{220}} + 69^{220^{119}} \;\vdots\; 102$;

b) $6^{2n+1} + 5^{n+2} \;\vdots\; 31$ $(n = 0, 1, 2, \ldots)$.

6.4. Hãy nghiên cứu dấu hiệu chia hết cho

2 ; 3 ; 4 ; 5 ; 6 ; 7 ; 8 ; 9 ; 11

của các số tự nhiên viết trong hệ ghi số thập phân.

6.5. Chứng minh rằng với m, n là hai số tự nhiên lẻ, ta có

$$1^n + 2^n + \ldots + m^n \equiv 0 \pmod{m}.$$

6.6. Cho p là một số tự nhiên lớn hơn 1. Chứng minh rằng các mệnh đề sau là tương đương :

a) p là số nguyên tố;

b) $C_p^k \equiv 0 \pmod p$, với mọi $k = 1, 2, \ldots, p-1$;

c) $C_{p-1}^k \equiv (-1)^k \pmod p$ với mọi $k = 0, 1, \ldots, p-1$.

6.7. Cho m và n là hai số tự nhiên khác không. Chứng minh rằng nếu $a \equiv b \pmod{m^n}$ thì $a^m \equiv b^m \pmod{m^{n+1}}$.

6.8. Chứng minh rằng

a) $2^{3^n} \equiv -1 \pmod{3^{n+1}}$, $n = 1, 2, \ldots$;

b) Có nhiều vô hạn số tự nhiên a thỏa mãn $a \mid 2^a + 1$.

6.9. Chứng minh rằng

a) Với m là một số tự nhiên lẻ > 1 cho trước ta có

$$(m-1)^{m^n} \equiv -1 \pmod{m^{n+1}}, \quad n = 1, 2, \ldots;$$

b) Có nhiều vô hạn số tự nhiên a thỏa mãn $a \mid 2^{2a} + 1$.

6.10. Cho $m_1, m_2, \ldots, m_k$ là những số tự nhiên lớn hơn 1 đôi một nguyên tố cùng nhau, b là một số nguyên tùy ý.

Đặt $m = m_1 m_2 \ldots m_k$ và $a_i = \dfrac{m}{m_i}$, $i = 1, 2, \ldots, k$.

a) Chứng minh rằng khi $x_1, x_2, \ldots, x_k$ lần lượt chạy qua các hệ thặng dư đầy đủ môđun m_1, môđun m_2, ..., môđun m_k thì $a_1x_1 + a_2x_2 + \ldots + a_kx_k + b$ chạy qua hệ thặng dư đầy đủ môđun m.

b) Chứng minh rằng khi $x_1, x_2, \ldots, x_k$ lần lượt chạy qua các hệ thặng dư thu gọn môđun m_1, môđun m_2, ..., môđun m_k thì $a_1x_1 + a_2x_2 + \ldots + a_kx_k$ chạy qua hệ thặng dư thu gọn môđun m.

6.11. Chứng minh rằng mỗi lớp thặng dư môđun m gồm và chỉ gồm k lớp thặng dư môđun km.

6.12. Chứng minh rằng nếu $(a, m) = 1$ và α, β là hai số tự nhiên sao cho $\alpha \equiv \beta \pmod{\varphi(m)}$ thì ta có $a^\alpha \equiv a^\beta \pmod m$.

6.13. Tìm số dư trong các phép chia

a) 6^{592} chia cho 11; b) 3^{40} chia cho 83; c) $5^{70} + 7^{50}$ chia cho 12; d) $3.5^{75} + 4.7^{100}$ chia cho 132; e) 35^{150} chia cho 425; g) $10^{10} + 10^{10^2} + \ldots + 10^{10^{10}}$ chia cho 7.

6.14. a) Tìm hai chữ số tận cùng bên phải của các số sau đây viết trong hệ ghi cơ số thập phân:

$$2^{999} \; ; \; 3^{5^{1977}} \; ; \; 14^{14^{14}}$$

b) Chứng minh rằng hai chữ số tận cùng bên phải (viết trong hệ ghi cơ số thập phân) của 9^{9^9} và $9^{9^{9^9}}$ là như nhau.

6.15. Chứng minh rằng

a) $2^{70} + 3^{70} \vdots 13$; b) $20^{15} - 1 \vdots 11.31.61$; c) $2^{3^{4n+1}} + 3 \vdots 11$ $(n = 0, 1, 2, \ldots)$; d) $2^{2^{6n+2}} + 3 \vdots 19$ $(n = 0, 1, 2, \ldots)$; e) $2^{n!} - 1 \vdots n$ (với n là số tự nhiên lẻ).

6.16. Chứng minh rằng

a) Với $(a, 240) = 1$ ta có $a^4 - 1 \vdots 240$;

b) Với $(a, 5) = 1$ ta có $a^{8n} + 3a^{4n} - 4 \vdots 100$;

c) Với số nguyên tố $p > 7$ ta có $3^p - 2^p - 1 \vdots 42p$.

6.17 a) Tìm tất cả các số tự nhiên n sao cho $n \mid 2^n - 1$.

b) Tìm tất cả các số nguyên tố p sao cho $p \mid 2^p + 1$.

6.18. Cho m và n là hai số tự nhiên lớn hơn 1 nguyên tố cùng nhau. Chứng minh rằng

$$m^{\varphi(n)} + n^{\varphi(m)} \equiv 1 \pmod{mn}.$$

6.19. Cho p là một số nguyên tố lẻ. Chứng minh rằng với hai số tự nhiên m, n khác 0, ta có

$a^{m(p-1)} + a^{n(p-1)} \not\equiv 0 \pmod p$ khi và chỉ khi $a \equiv 0 \pmod p$.

6.20. Chứng minh rằng nếu $a_1 + a_2 + \ldots + a_n \equiv 0 \pmod{30}$, thì

$$a_1^5 + a_2^5 + \ldots + a_n^5 \equiv 0 \pmod{30}.$$

6.21. Chứng minh rằng

a) $1^{30} + 2^{30} + \ldots + 10^{30} \equiv -1 \pmod{11}$;

b) Với p là một số nguyên tố lẻ ta có:

$1^m + 2^m + \ldots + (p-1)^m \equiv -1 \pmod p$ nếu $m \equiv 0 \pmod{(p-1)}$;

$1^m + 2^m + \ldots + (p-1)^m \equiv 0 \pmod p$ nếu $m \not\equiv 0 \pmod{(p-1)}$.

6.22. Cho p là một số nguyên tố lẻ. Chứng minh rằng

a) $a^{p-1} + a^{p-2} + \ldots + a + 1 \not\equiv 0 \pmod{p^2}$;

b) $a \equiv 1 \pmod{p^r}$ khi và chỉ khi $a^p \equiv 1 \pmod{p^{r+1}}$.

6.23. Chứng minh rằng

a) Với các số tự nhiên a lớn hơn b và n lớn hơn 1 thì mỗi ước nguyên tố của $a^n - b^n$ hoặc là ước của $a^s - b^s$ với s là ước thực sự của n, hoặc có dạng nk+1.

b) Với số nguyên tố p>2 thì ước nguyên tố của $a^p - 1$ hoặc là ước của a−1 (a ≠ 1) hoặc có dạng 2pk+1. Đặc biệt, ta có ước nguyên tố của số $M_p = 2^p - 1$ (p là số nguyên tố lẻ) có dạng 2pk+1.

6.24. Chứng minh rằng:

a) Với các số tự nhiên a, b và n > 1 thì mỗi ước nguyên tố của $a^n + b^n$ hoặc là ước của $a^s + b^s$ với s là ước thực sự của n, hoặc là có dạng 2nk+1.

b) Với số nguyên tố p > 2 thì ước nguyên tố của $a^p + 1$ hoặc là ước của a+1 hoặc có dạng 2pk+1.

6.25. Chứng minh rằng:

a) Nếu a và b là hai số tự nhiên khác 0, nguyên tố cùng nhau thì mỗi ước nguyên tố lẻ của $a^2 + b^2$ phải có dạng 4m+1.

b) Nếu a và b là hai số tự nhiên khác 0, nguyên tố cùng nhau thì mỗi ước nguyên tố lẻ của $a^2 + b^2$ phải có dạng $2^{s+1}m + 1$.

6.26. Chứng minh rằng

a) Có nhiều vô hạn số nguyên tố dạng 2pk+1 (p là một số nguyên tố lẻ cho trước).

b) Có nhiều vô hạn số nguyên tố dạng $2^{s+1}k + 1$ (s là một số tự nhiên cho trước).

6.27. Cho p là một số nguyên tố và $h_1, h_2, \ldots, h_a$ là những số tự nhiên khác 0.

a) Chứng minh rằng ta có:

$$(h_1 + h_2 + \ldots + h_a)^p \equiv (h_1^p + h_2^p + \ldots + h_a^p) \pmod{p}.$$

b) Từ kết quả câu a) suy ra định lý Phécma.

c) Từ định lý Phécma ở câu b) suy ra định lý Ole.

BÀI THỨ BẢY

PHƯƠNG TRÌNH ĐỒNG DƯ

§1. PHƯƠNG TRÌNH ĐỒNG DƯ VÀ NGHIỆM CỦA PHƯƠNG TRÌNH ĐỒNG DƯ

1 – PHƯƠNG TRÌNH ĐỒNG DƯ MỘT ẨN

1. Định nghĩa. Phương trình đồng dư một ẩn là một đồng dư thức có dạng

$$f(x) = a_0x^n + a_1x^{n-1} + \ldots + a_{n-1}x + a_n \equiv 0 \pmod{m}, \quad (1)$$

trong đó m, n là những số tự nhiên khác không. Các số nguyên $a_0, a_1, \ldots, a_n$ được gọi là các hệ số, x được gọi là ẩn của phương trình đồng dư.

– Nếu với số nguyên $x = x_0$ ta có đồng dư thức bằng số

$$f(x_0) \equiv 0 \pmod{m},$$

thì ta nói rằng *phương trình (1) nghiệm đúng với* $x = x_0$, hay là $x = x_0$ *nghiệm đúng phương trình (1).*

Ví dụ. $x = 5$ nghiệm đúng phương trình $x^2 + 1 \equiv 0 \pmod{13}$ vì ta có $5^2 + 1 = 26 \equiv 0 \pmod{13}$.

–*Giải một phương trình đồng dư* là tìm tập hợp các giá trị nghiệm đúng phương trình đồng dư đó.

2. Phương trình đồng dư tương đương.

– Ta nói hai phương trình đồng dư

$$g(x) \equiv 0 \pmod{m_1},$$

và
$$h(x) \equiv 0 \pmod{m_2}$$

là *tương đương với nhau* nếu như tập hợp các giá trị nghiệm đúng phương trình này trùng với tập hợp các giá trị nghiệm đúng phương trình kia.

— Bằng cách biến đổi tương đương, ta có thể đưa việc giải phương trình đồng dư đã cho về giải phương trình đồng dư đơn giản hơn tương đương với nó.

Ví dụ. Phương trình

$$(x^2 + 1)(3x^2 + 6) \equiv 0 \pmod 9$$

tương đương với phương trình

$$x^2 + 2 \equiv 0 \pmod 3$$

hay là

$$x \equiv \pm 1 \pmod 3.$$

Thật vậy, giả sử với số nguyên $x = x_o$ ta có

$$(x_o^2 + 1)(3x_o^2 + 6) \equiv 0 \pmod 9.$$

Chia cả hai vế và môđun của đồng dư thức cho 3 ta được

$$(x_o^2 + 1)(x_o^2 + 2) \equiv 0 \pmod 3).$$

Nhưng $x_o^2 + 1$ không chia hết cho 3 và 3 là một số nguyên tố nên $(x_o^2 + 1, 3) = 1$, từ đó sau khi chia cả hai vế của đồng dư thức ở trên cho $x_o^2 + 1$ ta được

$$x_o^2 + 2 \equiv 0 \pmod 3$$

hay là

$$x_o^2 - 1 \equiv 0 \pmod 3,$$

$$(x_o + 1)(x_o - 1) \equiv 0 \pmod 3.$$

Do 3 là một số nguyên tố nên ta có hoặc $x_o - 1 \equiv 0$ (mod3) hoặc $x_o + 1 \equiv 0$ (mod3) tức là hoặc $x_o \equiv 1$ (mod3) hoặc $x_o \equiv -1$ (mod3).

Ngược lại giả sử số nguyên $x = x_o$ thỏa mãn hoặc $x_o \equiv 1$ (mod3) hoặc $x_o \equiv -1$ (mod3) khi ấy dựa vào các tính chất của đồng dư thức ta được

$$x_o^2 \equiv 1 \pmod{3}$$

hay
$$x_o^2 + 2 \equiv 0 \pmod{3},$$

từ đó
$$(x_o^2 + 1)\ (3x_o^2 + 6) \equiv 0 \pmod{3}.$$

3. Bậc của phương trình đồng dư

—Trong phương trình (1) ta có thể giả thiết a_o không chia hết cho m. bởi vì nếu $a_o \equiv 0 \pmod{m}$ thì ta có thể bỏ số hạng $a_o x^n$ ở phương trình (1) đi và ta được một phương trình tương đương.

— Trong phương trình (1) ta có thể đưa các hệ số a_o $a_1, \ldots, a_n$ về các số nguyên không âm nhỏ thua m.

— Trong phương trình (1) nếu $a_o \not\equiv 0 \pmod{m}$ thì ta nói rằng n là *bậc của phương trình đồng dư (1).*

Ví dụ. Phương trình $12x^5 - 7x^4 + x^2 + 6x + 8 \equiv 0 \pmod{3}$ có thể viết dưới dạng

$3 \cdot 4x^5 + 3(-3)\,x^4 + 2x^4 + x^2 + 3 \cdot 2x + 3 \cdot 2 + 2 \equiv 0 \pmod{3}$ nên phương trình đã cho tương đương với phương trình

$$2x^4 + x^2 + 2 \equiv 0 \pmod{3}$$

và bậc của nó là $n = 4$.

II—HỆ PHƯƠNG TRÌNH ĐỒNG DƯ MỘT ẨN

1. Cho hệ k phương trình đồng dư một ẩn

$$\begin{cases} f_1(x) \equiv 0 \pmod{m_1}, \\ f_2(x) \equiv 0 \pmod{m_2}, \\ \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \\ f_k(x) \equiv 0 \pmod{m_k}. \end{cases} \qquad (I)$$

Nếu với số nguyên $x = x_o$ ta có k đồng dư thức bằng số $f_i(x_o) \equiv 0 \pmod{m_i}$, $i = 1, 2, \ldots, k$

thì ta nói x_o *nghiệm đúng hệ phương trình (I).*

— *Giải một hệ phương trình đồng dư là tìm tập hợp các giá trị nghiệm đúng* hệ phương trình đồng dư đó.

2. *Cho hệ gồm l phương trình đồng dư*

$$\begin{cases} g_1(x) \equiv 0 \pmod{m'_1}, \\ g_2(x) \equiv 0 \pmod{m'_2}, \\ \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \\ g_l(x) \equiv 0 \pmod{m'_l}. \end{cases} \qquad (II)$$

Ta nói hệ phương trình (I) và hệ phương trình (II) là *tương đương* với nhau nếu tập hợp các giá trị nghiệm đúng hệ phương trình (I) trùng với tập hợp các giá trị nghiệm đúng hệ phương trình (II).

Ví dụ. Phương trình

$$(x^2 + 1)(x^2 + 2) \equiv 0 \pmod{15}$$

tương đương với hệ phương trình

$$\begin{cases} x^2 + 1 \equiv 0 \pmod 5, \\ x^2 + 2 \equiv 0 \pmod 3. \end{cases}$$

Thật vậy, giả sử với số nguyên $x = x_o$ ta có

$$(x_o^2 + 1)(x_o^2 + 2) \equiv 0 \pmod{15}$$

thì ta cũng có (7 . II, §1. B.6)

$(x_o^2 + 1)(x_o^2 + 2) \equiv 0 \pmod 5$ và $(x_o^2 + 1)(x_o^2 + 2) \equiv 0 \pmod 3$ lại vì $(x_o^2 + 2, 5) = 1$ nên từ $(x_o^2 + 1)(x_o^2 + 2) \equiv 0 \pmod 5$ ta được $x_o^2 + 1 \equiv 0 \pmod 5$ (4 . II, §1. B.6).

Tương tự như vậy ta cũng có $x_o^2 + 2 \equiv 0 \pmod 3$ bởi vì $(x_o^2 + 1)(x_o^2 + 2) \equiv 0 \pmod 3$ và $(x_o^2 + 1, 3) = 1$.

Ngược lại giả sử với số nguyên $x = x_o$ ta có

$$x_o^2 + 1 \equiv 0 \pmod 5$$

và

$$x_o^2 + 2 \equiv 0 \pmod 3.$$

Khi ấy ta cũng có (3 . d) II §1. B.6)

$$(x_o^2 + 1)(x_o^2 + 2) \equiv 0 \pmod 5$$

và $$(x_o^2 + 1)(x_o^2 + 2) \equiv 0 \pmod 3.$$

Từ hai đồng dư thức này và do 3 và 5 là nguyên tố cùng nhau ta được (6.II §1. B.6)

$$(x_o^2 + 1)(x_o^2 + 2) \equiv 0 \pmod{15}.$$

III – NGHIỆM CỦA MỘT PHƯƠNG TRÌNH ĐỒNG DƯ VÀ NGHIỆM CỦA MỘT HỆ PHƯƠNG TRÌNH ĐỒNG DƯ

1. Nghiệm của một phương trình đồng dư

a) Ta biết rằng *nếu số nguyên $x = x_o$ nào đó nghiệm đúng phương trình (1) thì tất cả các số nguyên thuộc lớp $x \equiv x_o$ (mođm)* tức là tất cả các số nguyên có dạng $x = x_o + km$ ($k \in \mathbb{Z}$) *đều nghiệm đúng phương trình (1)* (3 g, II §.1. B.6). Khi ấy ta nói lớp $x \equiv x_o$ (modm) là một nghiệm của phương trình đồng dư (1).

Vậy nếu số nguyên x_o nghiệm đúng phương trình (1) thì ta nói lớp thặng dư $\overline{x_o}$ (modm) là *một nghiệm của phương trình (1).*

b) Hệ quả. *Số nghiệm của một phương trình đồng dư theo môđun m không vượt quá m.*

Điều này là hiển nhiên bởi vì Z_m có m phần tử.

Như vậy để tìm nghiệm của một phương trình đồng dư ta chỉ việc lần lượt cho x lấy các giá trị của một

hệ thặng dư đầy đủ và thử xem giá trị nào nghiệm đúng phương trình đã cho.

Ví dụ.

Bằng cách thử qua hệ thặng dư đầy đủ $\{0, \pm 1, \pm 2\}$ ta thấy phương trình

$$x^3 + 1 \equiv 0 \pmod{5}$$

có nghiệm duy nhất là

$$x \equiv -1 \pmod{5}.$$

Bằng cách thử qua hệ thặng dư đầy đủ $\{0, \pm 1, \pm 2, 3\}$ ta thấy phương trình

$$x^3 - x + 1 \equiv 0 \pmod{6}$$

không có nghiệm.

2. Nghiệm của một hệ phương trình đồng dư.

a) *Nếu số nguyên $x = x_0$ nghiệm đúng hệ phương trình (I) thì tất cả các số nguyên thuộc lớp* $\overline{x}_0$ (mod$m$) trong đó $m = [m_1, m_2, \ldots, m_k]$, *đều nghiệm đúng hệ phương trình (I).*

Thật vậy, nếu $f_i(x_0) \equiv 0 \pmod{m_i}$, $i = 1, 2, \ldots, k$ thì $f_i(x_0) \equiv 0 \pmod{m}$, $i = 1, 2, \ldots, k$ (6.II.§ 1. B.6). Từ đó với số nguyên t tùy ý ta có (3g.II. § 1, B.6)

$$f_i(x_0 + mt) \equiv 0 \pmod{m},\ i = 1, 2, \ldots, k,$$

suy ra

$$f_i(x_0 + mt) \equiv 0 \pmod{m_i},\ i = 1, 2, \ldots, k.$$

Điều này chứng tỏ rằng tất cả các số nguyên thuộc lớp $\overline{x}_0$ (mod$m$) đều nghiệm đúng hệ phương trình (I).

— Nếu số nguyên x_0 nghiệm đúng hệ phương trình (I) thì ta nói lớp thặng dư $\overline{x}_0$ (mod$m$) (trong đó $m = [m_1, m_2, \ldots, m_k]$ là *một nghiệm của hệ phương trình đồng dư (I).*

Ví dụ $x \equiv 2 \pmod{15}$ là một nghiệm của hệ phương trình

$$\begin{cases} x^2 + 1 \equiv 0 \pmod{5}, \\ x^2 + 2 \equiv 0 \pmod{3}. \end{cases}$$

IV – PHƯƠNG TRÌNH ĐỒNG DƯ VÀ PHƯƠNG TRÌNH VÔ ĐỊNH

Phương trình đồng dư thực chất là phương trình vô định, điều này được cụ thể hóa bởi mệnh đề sau đây:

Giả sử $f(x) = a_0 x^n + a_1 x^{n-1} + \dots + a_n$ là một đa thức với hệ số nguyên, b là một số nguyên khác không. Khi ấy hiển nhiên rằng phương trình vô định

$$f(x) + by = 0$$

tương đương với hệ

$$\begin{cases} f(x) \equiv 0 \pmod{|b|}, \\ y = \dfrac{f(x)}{-b}. \end{cases}$$

Ví dụ. Phương trình vô định

$$x^3 + 5y + 1 = 0$$

tương đương với hệ

$$\begin{cases} x^3 + 1 \equiv 0 \pmod{5}, \\ y = \dfrac{x^3 + 1}{-5}. \end{cases}$$

Phương trình đồng dư $x^3 + 1 \equiv 0 \pmod{5}$ có nghiệm duy nhất là $x \equiv -1 \pmod{5}$, tức là tất cả các số nguyên $x = -1 + 5t$, $t = 0, \pm 1, \dots$ nên phương trình vô định $x^3 + 5y + 1 = 0$ có nghiệm là

$$\begin{cases} x = -1 + 5t, \\ y = \dfrac{(-1+5t)^3 + 1}{-5} = -3t + 15t^2 - 25t^3 \end{cases}$$

với $t = 0, \pm 1, \dots$

§2. PHƯƠNG TRÌNH ĐỒNG DƯ BẬC NHẤT MỘT ẨN

Trong tiết này chúng ta xét phương trình đồng dư bậc nhất một ẩn dạng

$$ax \equiv b \pmod{m} \qquad (1)$$

dĩ nhiên ở đó $a \not\equiv 0 \pmod{m}$.

1. *Phương trình (1) có nghiệm khi và chỉ khi $d \mid b$, trong đó $d = (a, m)$.*

Chứng minh. Giả sử số nguyên x_0 nghiệm đúng phương trình (1), nghĩa là $ax_0 \equiv b \pmod{m}$. Từ $d = (a, m)$ ta có $d \mid ax_0$. Nhưng tập hợp các ước chung của ax_0 với m trùng với tập hợp các ước chung của b với m cho nên do $d \mid ax_0$ và $d \mid m$ ta có $d \mid b$.

Ngược lại giả sử $d \mid b$ nghĩa là $b = b_1 d$ với b_1 là một số nguyên nào đó. Khi ấy từ giả thiết $d = (a,m)$ ắt có cặp số nguyên x_1, y_1 sao cho $ax_1 + my_1 = d$, nghĩa là $ax_1 \equiv d \pmod{m}$. Từ đây ta có

$$ab_1x_1 \equiv db_1 \pmod{m}$$

hay là

$$a(b_1x_1) \equiv b \pmod{m}.$$

Đồng dư thức sau cùng này chứng tỏ $x_0 = b_1 x_1$ nghiệm đúng phương trình (1).

2. *Nếu $(a,m) = 1$ thì phương trình (1) có nghiệm duy nhất.*

Chứng minh. Thật vậy, ta cho x chạy qua một hệ thặng dư đầy đủ môđun m; khi ấy vì $(a,m) = 1$ nên ax cũng chạy qua một hệ thặng dư đầy đủ môđun m, do đó ắt có duy nhất số nguyên x_0 sao cho ax_0 cùng lớp với b theo môđun m, nghĩa là

$$ax_0 \equiv b \pmod{m}.$$

Vậy phương trình (1) có nghiệm duy nhất là $x \equiv x_0 \pmod{m}$.

3. *Nếu $(a,m) = d > 1$ và $d \mid b$ thì phương trình (1) có đúng d nghiệm.*

Chứng minh. Từ giả thiết $(a,m) = d$ và $d \mid b$ ta có $a = a_1 d$, $m = m_1 d$ với $(a_1, m_1) = 1$ và $b = b_1 d$. Khi ấy phương trình (1) tương đương với phương trình $a_1 x \equiv b_1 \pmod{m_1}$. Bởi vì $(a_1, m_1) = 1$ nên phương trình $a_1 x \equiv b_1 \pmod{m_1}$ có nghiệm duy nhất, chẳng hạn là

$$x \equiv x_0 \pmod{m_1}.$$

Nhưng trong lớp thặng dư $x \equiv x_0 \pmod{m_1}$ có đúng d nghiệm của phương trình (1) là d lớp thặng dư theo môđun m xác định như sau:

$$x \equiv x_0 \qquad \pmod{m},$$
$$x \equiv x_0 + m_1 \qquad \pmod{m},$$
$$x \equiv x_0 + 2m_1 \qquad \pmod{m},$$
$$\dots\dots\dots$$
$$x \equiv x_0 + (d-1)\, m_1 \qquad \pmod{m}.$$

Thật vậy, giả sử α là một thặng dư nào đó thuộc lớp $x \equiv x_0 \pmod{m_1}$ nghĩa là $\alpha \equiv x_0 \pmod{m_1}$. Khi đó ắt có số nguyên t sao cho $\alpha = x_0 + m_1 t$. Bằng cách chia t cho d, chẳng hạn ta được $t = dq + r$, $0 \leqslant r < d$, khi đó $\alpha = x_0 + m_1 r + (m, d) q = x_0 + m_1 r + mq$ hay là $\alpha \equiv x_0 + m_1 r \pmod{m}$ nói khác đi α thuộc lớp $x \equiv x_0 + m_1 r \pmod{m}$ với r nào đó $(0 \leqslant r \leqslant d-1)$.

Ngược lại giả sử α thuộc lớp $x \equiv x_0 + km_1 \pmod{m}$ với k nào đó $(0 \leqslant k \leqslant d-1)$ nghĩa là $\alpha \equiv x_0 + km_1 \pmod{m}$. Khi đó ta cũng có $\alpha \equiv x_0 + km_1 \pmod{m_1}$ vì m_1 là ước của m, do đó $\alpha \equiv x_0 \pmod{m_1}$, nói khác đi α thuộc lớp $x \equiv x_0 \pmod{m_1}$.

Hơn nữa với $k \neq l$ $(0 \leqslant k, l \leqslant d-1)$ ta có

$$km_1 \neq lm_1 \; (0 \leqslant km_1,\, lm_1 < m) \text{ nên}$$

$$x_0 + km_1 \not\equiv x_0 + lm_1 \pmod{m}.$$

Vậy ta đã chứng minh được rằng phương trình (1) có đúng d nghiệm nếu như $(a, m) = d > 1$ và $d \mid b$.

Ví dụ. Phương trình $10x \equiv 15 \pmod{35}$ có $(10,35) = 5 \mid 15$ nên nó có 5 nghiệm. Cụ thể là phương trình đã cho tương đương với phương trình $2x \equiv 3 \pmod{7}$ mà phương trình $2x \equiv 3 \pmod{7}$ có nghiệm duy nhất là $x \equiv 5 \pmod{7}$ nên phương trình đã cho $10x \equiv 15 \pmod{35}$ có 5 nghiệm là

$$x \equiv 5,\ 12,\ 19,\ 26,\ 33 \pmod{35}.$$

4. *Cách xác định nghiệm của phương trình* (1).

Ta chỉ cần xét trường hợp phương trình $ax \equiv b \pmod{m}$ với điều kiện a và m nguyên tố cùng nhau.

a) *Cách thứ nhất.* Chia cả hai vế cho a.

— Nếu $a \mid b$ thì ta được nghiệm của phương trình (1) là

$$x \equiv \frac{b}{a} \pmod{m}.$$

— Nếu a không chia hết b thì do $(a,m) = 1$ ắt có số nguyên k, $1 \leqslant k \leqslant a - 1$ để $b + km$ là bội của a, từ đó phương trình (1) có nghiệm là

$$x \equiv \frac{b + km}{a} \pmod{m}.$$

Ví dụ. Giải phương trình $3x \equiv 1 \pmod{7}$.

Phương trình đã cho tương đương với phương trình $3x \equiv 1 + 2.7 \pmod{7}$, nên ta có $x \equiv \dfrac{1 + 2.7}{3} \pmod{7}$ hay là $x \equiv 5 \pmod{7}$ là nghiệm của phương trình đã cho.

Cách xác định nghiệm như trên là đơn giản song chỉ tiến hành được trong trường hợp dễ dàng thấy ngay k hoặc trong trường hợp a là những số nhỏ.

b) *Cách thứ hai.* Dựa vào định lý Ơle.

Từ giả thiết $(a,m) = 1$, theo định lý Ơle ta có

$$a^{\varphi(m)} \equiv 1 \pmod{m}.$$

Nhân cả hai vế đồng dư thức này với b ta có thể viết

$$a\,(ba^{\varphi(m)-1}) \equiv b \pmod{m}.$$

Điều này chứng tỏ rằng phương trình (1) có nghiệm là

$$x \equiv ba^{\varphi(m)-1} \pmod{m}.$$

Ví dụ. Giải phương trình $5x \equiv 3 \pmod{9}$.

Phương trình đã cho có nghiệm là

$$x \equiv 5^{\varphi(9)-1} \,.\, 3 \pmod{9}$$

$$x \equiv 5^{5}.3 \pmod{9}.$$

$$5^2 \equiv -2 \pmod{9}\ ,\ 5^3 \equiv -1 \pmod{9},\ 5^5 \equiv 2 \pmod{9}.$$

$5^5 \cdot 3 \equiv 6 \pmod{9}$. Vậy nghiệm của phương trình đã cho chính là $x \equiv 6 \pmod{9}$.

c) *Cách thứ ba.* Dùng liên phân số.

Ngoài giả thiết $(a,m) = 1$, ta có thể giả thiết thêm rằng $1 < a < m$: sau khi khai triển $\frac{m}{a}$ thành liên phân số:

$$\frac{m}{a} = [q_0 ; q_1, \ldots, q_n] = \frac{P_n}{Q_n}$$

ta có $m = P_n$ và $a = Q_n$.

Theo tính chất của các giản phân thì

$$aP_{n-1} - mQ_{n-1} = (-1)^n$$

hay

$$aP_{n-1} \equiv (-1)^n \pmod{m}.$$

Nhân cả hai vế của đồng dư thức này với $(-1)^n b$ ta được

$$a\,[(-1)^n bP_{n-1}] \equiv b \pmod{m}.$$

Đồng dư thức này chứng tỏ rằng phương trình (1) có nghiệm là

$$x \equiv (-1)^n b P_{n-1} \pmod m.$$

Ví dụ. Giải phương trình $17x \equiv 3 \pmod{97}$.

Ta có $\frac{97}{17} = [5; 1, 2, 2, 2]$ và $P_{n-1} = 40$ nên phương trình đã cho có nghiệm là

$$x \equiv (-1)^4 . 3 . 40 \pmod{97}$$

hay là $$x \equiv 23 \pmod{97}.$$

Như vậy là vấn đề phương trình đồng dư bậc nhất đã được giải quyết hoàn toàn. Ta đã biết phương trình đồng dư $ax \equiv b \pmod m$ có thể coi là phương trình vô định $ax + my = b$ mà ở đây ta chỉ lưu ý đến ẩn x mà thôi.

§3. HỆ PHƯƠNG TRÌNH ĐỒNG DƯ BẬC NHẤT MỘT ẨN

Trong tiết này chúng ta sẽ xét một hệ gồm k phương trình bậc nhất một ẩn dạng

$$\begin{cases} x \equiv b_1 \pmod{m_1}, \\ x \equiv b_2 \pmod{m_2}, \\ \quad \dots\dots \\ x \equiv b_k \pmod{m_k}. \end{cases} \qquad (I)$$

Có thể nói rằng việc giải các hệ phương trình dạng (I) là bước cuối cùng của việc giải một phương trình đồng dư hay một hệ phương trình đồng dư. Để cho tiện ta gọi m là bội chung nhỏ nhất của các môđun $m_1, m_2, \dots, m_k$ và gọi d_{ij} là ước chung lớn nhất của các cặp môđun m_i, m_j với mọi $i, j = 1, 2, \dots, k$.

1. *Nếu hệ phương trình (I) có nghiệm thì nó có nghiệm duy nhất.*

Chứng minh. Thật vậy, giả sử α, β nghiệm đúng hệ phương trình (I) nghĩa là ta có

$$\alpha \equiv b_i \pmod{m_i},\ i = 1, 2, \ldots, k$$

và $$\beta \equiv b_i \pmod{m_i},\ i = 1, 2, \ldots, k$$

cho nên $\alpha \equiv \beta \pmod{m_i}$, $i = 1, 2, \ldots, k$. Từ đó suy ra rằng $$\alpha \equiv \beta \pmod{m}.$$

Vậy các nghiệm $x \equiv \alpha \pmod{m}$ và $x \equiv \beta \pmod{m}$ của hệ phương trình (I) là trùng nhau.

2. *Nếu hệ phương trình (I) có nghiệm thì d_{ij} là ước của $b_i - b_j$ với mọi $i, j = 1, 2, \ldots, k$.*

Chứng minh. Giả sử hệ phương trình (I) có nghiệm là $x \equiv x_0 \pmod{m}$ nghĩa là ta có

$$x_0 \equiv b_i \pmod{m_i},\ i = 1, 2, \ldots, k.$$

Xét hai đồng dư thức trong k đồng dư thức này là

$$x_0 \equiv b_i \pmod{m_i},\ \text{và}\ x_0 \equiv b_j \pmod{m_j}.$$

Bởi vì $(m_i, m_j) = d_{ij} > 0$ nên từ hai đồng dư thức trên ta cũng có (7. II. § 1, B. 6):

$$x_0 \equiv b_i \pmod{d_{ij}}$$

và $$x_0 \equiv b_j \pmod{d_{ij}}.$$

Từ đó suy ra $b_i - b_j \equiv 0 \pmod{d_{ij}}$ (2.II. § 1. B.6), nghĩa là $d_{ij} \mid b_i - b_j$.

3. *Nếu $m_1, m_2, \ldots, m_k$ nguyên tố cùng nhau từng đôi một thì hệ phương trình (I) có nghiệm.*

Chứng minh. Giả thiết $d_{ij} = (m_i, m_j) = 1$, $i \neq j$ i, $j = 1, 2, \ldots, k$ ta sẽ chứng minh rằng hệ phương trình (I) có nghiệm bằng phép qui nạp toán học theo k.

Xét hệ hai phương trình

$$\begin{cases} x \equiv b_1 \pmod{m_1}, \\ x \equiv b_2 \pmod{m_2} \end{cases}$$

với $(m_1, m_2) = 1$.

Hệ hai phương trình này tương đương với hệ

$$\begin{cases} x = b_1 + m_1 t, \\ b_1 + m_1 t \equiv b_2 \pmod{m_2} \end{cases}$$

với t là một số nguyên.

Bởi vì $(m_1, m_2) = 1$ nên phương trình

$$m_1 t \equiv b_2 - b_1 \pmod{m_2}$$

có nghiệm, giả sử là $t \equiv t_0 \pmod{m_2}$ tức là $t = t_0 + m_2 u$ với u là một số nguyên tùy ý. Thay giá trị của t vào biểu thức của x ta được

$x = b_1 + m_1(t_0 + m_2 u) = b_1 + m_1 t_0 + m_1 m_2 u$, với $u = 0, \pm 1, \pm 2, \ldots$ Vậy hệ hai phương trình ở trên có nghiệm là:

$$x \equiv x_2 \pmod{m_1 m_2}, \text{ ở đó } x_2 = b_1 + m_1 t_0.$$

Bây giờ giả sử mệnh đề đã đúng với số tự nhiên $s \geqslant 2$ ta phải chứng minh mệnh đề cũng đúng với số tự nhiên $s + 1$.

Thật vậy ta hãy xét hệ $s + 1$ phương trình

$$\begin{cases} x \equiv b_1 \pmod{m_1}, \\ x \equiv b_2 \pmod{m_2}, \\ \dots\dots\dots\dots \\ x \equiv b_s \pmod{m_s}, \\ x \equiv b_{s+1} \pmod{m_{s+1}}, \end{cases} \qquad (11)$$

trong đó $m_1, m_2, \ldots, m_s, m_{s+1}$ nguyên tố cùng nhau từng đôi một.

Theo giả thiết qui nạp, giả sử hệ s phương trình

$$\begin{cases} x \equiv b_1 \pmod{m_1}, \\ x \equiv b_2 \pmod{m_2}, \\ \dots\dots\dots\dots \\ x \equiv b_s \pmod{m_s} \end{cases}$$

có nghiệm là $x \equiv x_s \pmod{m_1 m_2 \ldots m_s}$. Khi ấy bởi vì $m_1, m_2, \ldots, m_s, m_{s+1}$ nguyên tố cùng nhau từng đôi một cho nên ta có thể thấy được rằng hệ phương trình (11) tương đương với hệ hai phương trình:

$$\begin{cases} x \equiv x_s \pmod{m_1 m_2 \ldots m_s}, \\ x \equiv b_{s+1} \pmod{m_{s+1}}. \end{cases}$$

Từ điều kiện $m_1, m_2, \ldots, m_s, m_{s+1}$ nguyên tố cùng nhau từng đôi một ta có tích $m_1 m_2 \ldots m_s$ nguyên tố với m_{s+1} cho nên hệ hai phương trình trên đây có nghiệm là $x \equiv x_{s+1} \pmod{m_1 m_2 \ldots m_s m_{s+1}}$ đó chính cũng là nghiệm của hệ phương trình (II). Định lý đã được chứng minh.

Ví dụ. Hệ phương trình

$$\begin{cases} x \equiv 2 \pmod{3}, \\ x \equiv 3 \pmod{5}, \\ x \equiv 2 \pmod{7}, \end{cases}$$

có nghiệm là $x \equiv 23 \pmod{105}$.

4. *Nếu d_{ij} là ước của $b_i - b_j$ với mọi $i, j = 1, 2, \ldots, k$ thì hệ phương trình (I) có nghiệm.*

Chứng minh. Ta sẽ chứng minh rằng hệ phương trình (I) tương đương với một hệ phương trình bậc nhất mà các môđun nguyên tố cùng nhau từng đôi một. Giả sử bội chung nhỏ nhất $m = [m_1, m_2, \ldots, m_k]$ của các môđun $m_1, m_2, \ldots, m_k$ có dạng phân tích tiêu chuẩn là $m = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_r^{\alpha_r}$. Khi ấy các môđun m_t $(1 \leqslant t \leqslant k)$ có thể viết dưới dạng

$$m_t = p_1^{\beta_{t1}} p_2^{\beta_{t2}} \ldots p_r^{\beta_{tr}}, \ t = 1, 2, \ldots, k$$

$$0 \leqslant \beta_{tl} \leqslant \alpha_l, \ l = 1, 2, \ldots, r.$$

Với mỗi $t = 1, 2, \ldots, k$ phương trình $x \equiv b_t \pmod{m_t}$ tương đương với hệ phương trình

$$\begin{cases} x \equiv b_t \pmod{p_1^{\beta_{t1}}}, \\ x \equiv b_t \pmod{p_2^{\beta_{t2}}}, \\ \ldots\ldots\ldots\ldots \\ x \equiv b_t \pmod{p_r^{\beta_{tr}}}. \end{cases}$$

Bởi vậy hệ phương trình (I) tương đương với hệ gồm kr phương trình

$$\begin{cases} x \equiv b_1 \pmod{p_l^{\beta_{1l}}}, \\ x \equiv b_2 \pmod{p_l^{\beta_{2l}}}, \\ \dots\dots\dots\dots \\ x \equiv b_k \pmod{p_l^{\beta_{kl}}}, \ l = 1, 2, \dots, r. \end{cases} \qquad \text{(III)}$$

Trong hệ phương trình (III) với mỗi l $(1 \leqslant l \leqslant r)$ ta có một hệ gồm k phương trình mà tất cả các môđun đều là lũy thừa của cùng một số nguyên tố p_l. Ta hãy nghiên cứu hai phương trình tùy ý của hệ phương trình này.

$$\begin{cases} x \equiv b_i \pmod{p_l^{\beta_{il}}}, \\ x \equiv b_j \pmod{p_l^{\beta_{jl}}}, \end{cases} \qquad \text{(IV)}$$

trong đó giả sử $\beta_{jl} \leqslant \beta_{il}$, $1 \leqslant i, j \leqslant k$.

Vì $d_{ij} = (m_i, m_j) \mid b_i - b_j$ nên ta cũng có $p_l^{\beta_{jl}} \mid b_i - b_j$ (do $p_l^{\beta_{jl}} = (p_l^{\beta_{jl}}, p_l^{\beta_{il}})$ là ước của d_{ij}. Từ đó ta có

$$b_i \equiv b_j \pmod{p_l^{\beta_{jl}}}.$$

Như vậy mọi số nghiệm đúng phương trình thứ nhất của hệ (IV) cũng nghiệm đúng phương trình thứ hai của nó, do đó hệ phương trình (IV) tương đương với phương trình thứ nhất của nó. Nói một cách khác với mỗi l $(1 \leqslant l \leqslant r)$ hai phương trình bất kỳ (trong hệ k phương trình ứng với l ấy) tương đương với phương trình có môđun lớn hơn, do đó hệ phương trình này ứng với l cố định $(1 \leqslant l \leqslant r)$ tương đương với phương trình có môđun lớn nhất trong hệ đó, môđun lớn nhất đó chính là $p_l^{\alpha_l}$, giả sử đó là phương trình

$$x \equiv x_l \pmod{p_l^{\alpha_l}},$$

với x_l là một b_t nào đó $t = 1, 2, \ldots, k$).

Ta lập luận như vậy với mọi $l = 1, 2, \ldots, r$, kết quả sẽ là hệ phương trình (I) tương đương với hệ phương trình

$$\begin{cases} x \equiv x_1 \pmod{p_1^{\alpha_1}}, \\ x \equiv x_1 \pmod{p_2^{\alpha_2}}, \\ \cdots\cdots\cdots \\ x \equiv x_r \pmod{p_r^{\alpha_r}}, \end{cases}$$

trong đó các môđun $p_1^{\alpha_1}, p_2^{\alpha_2}, \ldots, p_r^{\alpha_r}$ nguyên tố cùng nhau từng đôi một. Hệ phương trình này theo kết quả ở điểm trên có nghiệm, do đó hệ phương trình (I) có nghiệm và mệnh đề được chứng minh.

5. *Cách thực hành để xác định nghiệm của hệ phương trình (I).*

a) Trước hết, ta hãy xét trường hợp hệ *hai phương trình*:

$$\begin{cases} x \equiv b_1 \pmod{m_1}, \\ x \equiv b_2 \pmod{m_2}. \end{cases}$$

với giả thiết $d_{12} = (m_1, m_2)$ là ước của $b_1 - b_2$.

Phương trình thứ nhất được thỏa mãn với tất cả các số nguyên $x = b_1 + m_1 t$ với $t \in Z$. Bây giờ ta hãy xác định các số nguyên t sao cho x cũng nghiệm đúng phương trình thứ hai, nghĩa là

$$x = b_1 + m_1 t \equiv b_2 \pmod{m_2}$$

Như vậy có thể nói hệ hai phương trình trên tương đương với hệ

$$\begin{cases} x = b_1 + m_1 t \\ b_1 + m_1 t \equiv b_2 \pmod{m_2}. \end{cases}$$

Vì $d_{12} = (m_1, m_2)$ là ước của $b_1 - b_2$ nên phương trình $b_1 + m_1 t \equiv b_2 \pmod{m_2}$ tương đương với phương trình

$$\frac{m_1}{d_{12}} t \equiv \frac{b_2 - b_1}{d_{12}} \left(\mathrm{mod}\ \frac{m_2}{d_{12}}\right).$$

Nhưng $\left(\frac{m_1}{d_{12}}, \frac{m_2}{d_{12}}\right) = 1$ nên phương trình đồng dư này cho ta nghiệm

$$t \equiv t_o \left(\mathrm{mod}\ \frac{m_2}{d_{12}}\right)$$

hay là

$$t = t_o + \frac{m_2}{d_{12}} u, \text{ với mọi } u \in Z.$$

Thay giá trị của t vào biểu thức tính x ta được tập hợp các giá trị của x nghiệm đúng hệ hai phương trình đang xét là

$$x = b_1 + m_1 \left(t_o + \frac{m_2}{d_{12}} u\right) = b_1 + m_1 t_o + \frac{m_1 m_2}{d_{12}} u$$

hay là $x = x_o + [m_1, m_2] u$, với $x_o = b_1 + m_1 t_o$. Vậy $x \equiv x_o \pmod{[m_1, m_2]}$ là nghiệm của hệ hai phương trình đang xét.

b) *Đối với trường hợp hệ gồm k phương trình* $(k > 2)$ thì ta bắt đầu giải hệ hai phương trình nào đó của hệ, rồi thay trong hệ phương trình đã cho hai phương trình đã giải bằng nghiệm tìm được, ta sẽ được hệ gồm k – 1 phương trình tương đương với hệ phương trình đã cho. Tiếp tục như vậy sau k – 1 bước ta sẽ được nghiệm phải tìm.

c) *Ví dụ*. Giải hệ phương trình

$$\begin{cases} x \equiv 5 \pmod{6}, \\ x \equiv 8 \pmod{15}, \\ x \equiv -1 \pmod{12}, \\ x \equiv 13 \pmod{35}. \end{cases}$$

— Hệ hai phương trình

$$\begin{cases} x \equiv 5 \pmod{6} \\ x \equiv 8 \pmod{15} \end{cases}$$

tương đương với hệ

$$\begin{cases} x = 8 + 15t, \\ 8 + 15t \equiv 5 \pmod{6}, \ t \in Z. \end{cases}$$

Phương trình $8 + 15t \equiv 5 \pmod{6}$ cho ta $3t \equiv -3 \pmod{6}$ hay là $t \equiv -1 \pmod{2}$. Vậy ta được nghiệm của hệ hai phương trình đang xét là

$$x \equiv 8 + 15(-1) \pmod{[6, 15]}$$

hay là

$$x \equiv -7 \pmod{30}.$$

Do đó hệ phương trình đã cho tương đương với hệ phương trình

$$\begin{cases} x \equiv -7 \pmod{30}, \\ x \equiv -1 \pmod{12}, \\ x \equiv 13 \pmod{35}. \end{cases}$$

Lại giải hệ hai phương trình

$$\begin{cases} x \equiv -7 \pmod{30}, \\ x \equiv -1 \pmod{12} \end{cases}$$

ta được nghiệm của nó là $x \equiv 23 \pmod{60}$ và do đó hệ phương trình đã cho tương đương với hệ phương trình

$$\begin{cases} x \equiv 23 \pmod{60}, \\ x \equiv 13 \pmod{35}. \end{cases}$$

— Giải hệ hai phương trình này ta được nghiệm của nó là $x \equiv 83 \pmod{420}$, đó đồng thời cũng là nghiệm của hệ phương trình đã cho.

Chúng ta nhận thấy rằng hệ phương trình

$$\begin{cases} x \equiv b_1 \pmod{m_1}, \\ x \equiv b_2 \pmod{m_2}, \\ \dots\dots\dots \\ x \equiv b_k \pmod{m_k} \end{cases}$$

thực chất là hệ phương trình nguyên

$$x = m_1t_1 + b_1 = m_2t_2 + b_2 = \ldots = m_kt_k + b_k,$$

trong đó $m_1, m_2, \ldots, m_k$ và $b_1, b_2, \ldots, b_k$ là những số nguyên cho trước và $m_1, m_2, \ldots, m_k$ là những số tự nhiên khác 0. Các kết quả vừa tìm được ở trên cho ta điều kiện cần và đủ để hệ phương trình nguyên

$$m_1t_1 + b_1 = m_2t_2 + b_2 = \ldots = m_kt_k + b_k \qquad (1)$$

có nghiệm nguyên là

$$d_{ij} = (m_i, m_j) \mid b_i - b_j$$

với mọi $i, j = 1, 2, \ldots, k$. Đồng thời với cách thực hành giải hệ phương trình (I) ta cũng có cách thực hành tìm nghiệm nguyên của hệ phương trình (1).

§4. PHƯƠNG TRÌNH ĐỒNG DƯ THEO MÔĐUN NGUYÊN TỐ

Nhận xét. Xét phương trình đồng dư

$$f(x) = a_0x^n + a_1x^{n-1} + \ldots + a_n \equiv 0 \pmod{m}, \qquad (1)$$

trong đó $a_0 \not\equiv 0 \pmod{m}$ và giả sử $m = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_k^{\alpha_k}$ là dạng phân tích tiêu chuẩn của môđun m.

*) *Phương trình (1) tương đương với hệ phương trình*

$$\begin{cases} f(x) \equiv 0 \pmod{p_1^{\alpha_1}}, \\ f(x) \equiv 0 \pmod{p_2^{\alpha_2}}, \\ \ldots\ldots\ldots\ldots \\ f(x) \equiv 0 \pmod{p_k^{\alpha_k}}. \end{cases} \qquad (I)$$

Thật vậy, giả sử số nguyên x_0 nghiệm đúng phương trình (1) nghĩa là $f(x_0) \equiv 0 \pmod{m}$, khi ấy ta cũng có

$f(x_0) \equiv 0 \pmod{p_i^{\alpha_i}}$, $i = 1, 2, \ldots, k$ vì $p_i^{\alpha_i}$ là ước của m.
Nói khác đi x_0 nghiệm đúng hệ phương trình (I). Ngược lại, nếu số nguyên x_0 nghiệm đúng hệ phương trình (I), nghĩa là ta có các đồng dư thức $f(x_0) \equiv 0 \pmod{p_i^{\alpha_i}}$, $i = 1, 2, \ldots, k$ thì ta cũng có $f(x_0) \equiv 0 \pmod{m}$ vì m là bội chung nhỏ nhất của $p_1^{\alpha_1}, p_2^{\alpha_2}, \ldots, p_k^{\alpha_k}$, tức là x_0 nghiệm đúng phương trình (1).

Như vậy việc giải phương trình (1) được đưa về việc giải phương trình dạng

$$f(x) \equiv 0 \pmod{p^\alpha},$$

trong đó p là một số nguyên tố và $\alpha \geq 1$; và cuối cùng là giải hệ phương trình bậc nhất một ẩn dạng

$$\begin{cases} x \equiv b_1 \pmod{p_1^{\alpha_1}}, \\ x \equiv b_2 \pmod{p_2^{\alpha_2}}, \\ \ldots \\ x \equiv b_k \pmod{p_k^{\alpha_k}}, \end{cases}$$

mà ta đã xét ở tiết trước (§ 3)

Ta chú ý rằng nếu một trong các phương trình của hệ (I) vô nghiệm thì hệ phương trình ấy và do đó cả phương trình (1) vô nghiệm. Còn nếu như mỗi phương trình $f(x) \equiv 0 \pmod{p_i^{\alpha_i}}$ có s_i nghiệm ($i = 1, 2, \ldots, k$) thì hệ phương trình (I) và do đó cả phương trình (1) có $S = s_1 . s_2 \ldots s_k$ nghiệm.

**) *Nếu số nguyên x_0 nghiệm đúng phương trình*

$$f(x) \equiv 0 \pmod{p^\alpha},\ \alpha > 1 \quad (2)$$

thì x_0 cũng nghiệm đúng các phương trình

$$f(x) \equiv 0 \pmod{p^\beta},\ \beta = 1, 2, \ldots, \alpha - 1.$$

Điều này là hiển nhiên và từ đó ta suy ra rằng khi giải phương trình (2) ta chỉ cần tìm các nghiệm của nó trong các lớp nghiệm của phương trình

$$f(x) \equiv 0 \pmod{p^{\alpha-1}}.$$

Đối với phương trình mới này ta lại áp dụng kết quả đó để đưa về phương trình với môdun $p^{\alpha-1}$ và cứ thế lần ngược mãi lên đến phương trình

$$f(x) \equiv 0 \pmod{p}.$$

Qua những điều nhận xét ở trên ta thấy rằng vấn đề cơ bản trong việc giải phương trình đồng dư còn lại là vấn đề giải phương trình đồng dư theo môdun nguyên tố p:

$$f(x) = a_0x^n + a_1x^{n-1} + \ldots + a_n \equiv 0 \pmod{p}, \qquad (3)$$

trong đó $a_0 \not\equiv 0 \pmod{p}$.

Đối với phương trình đồng dư theo môdun nguyên tố bậc $n \leqslant 2$ người ta có thể biết rõ khi nào nó có nghiệm, còn trong trường hợp tổng quát thì kết quả chưa được là bao. Trong tiết này chúng ta nêu lên vài điểm đơn giản về phương trình đồng dư theo mô đun nguyên tố.

1. *Phương trình (3) hoặc nghiệm đúng với mọi số nguyên hoặc tương đương với một phương trình có bậc nhỏ hơn p.*

Chứng minh. Thực hiện phép chia f(x) cho $x^p - x$ giả sử ta được

$$f(x) = (x^p - x)\ g(x) + r(x),$$

trong đó g(x), r(x) là những đa thức với hệ số nguyên, r(x) hoặc bằng không hoặc có bậc nhỏ hơn p. Phương trình (3) trở thành

$$(x^p - x)\ g(x) + r(x) \equiv 0 \pmod{p}.$$

Nhưng vì với mọi $x \in \mathbb{Z}$ ta đều có $x^p - x \equiv 0 \pmod{p}$ cho nên phương trình (3) tương đương với phương trình

$$r(x) \equiv 0 \pmod{p}$$

ở đó hoặc $r(x) = 0$ hoặc $r(x)$ có bậc nhỏ hơn p. Từ đó suy ra điều cần phải chứng minh.

Ví dụ. Xét phương trình

$$4x^8 + 2x^6 - x^5 - 4x^4 + x^2 + x + 2 \equiv 0 \pmod{5}.$$

Khi chia $4x^8 + 2x^6 - x^5 - 4x^4 + x^2 + x + 2$ cho $x^5 - x$ ta được thương là $g(x) = 4x^3 + 2x - 1$ và dư là $r(x) = 3x^2 + 2$ do đó phương trình đã cho tương đương với phương trình

$$3x^2 + 2 \equiv 0 \pmod{5}.$$

Chú ý. Theo định lý vừa chứng minh ở trên, trong phương trình (3) ta có thể giả thiết $n < p$. Hơn nữa ta còn có thể giả thiết $a_0 = 1$. Thật vậy bởi vì $(a_0, p) = 1$. nên ắt có số nguyên a sao cho $a_0 a \equiv 1 \pmod{p}$ và dĩ nhiên $(a, p) = 1$. Do đó sau khi nhân hai vế của phương trình (3) với a ta được một phương trình tương đương với phương trình (3) mà hệ số của x^n lúc này bằng 1.

Ví dụ. Xét phương trình

$$3x^2 + 2 \equiv 0 \pmod{5}.$$

Bởi vì $3 . 2 \equiv 1 \pmod{5}$ nên sau khi nhân hai vế của phương trình đã cho với 2 ta được một phương trình tương đương là

$$6x^2 + 4 \equiv 0 \pmod{5}$$

hay là

$$x^2 + 4 \equiv 0 \pmod{5}.$$

2. Phương trình đồng dư theo môđun nguyên tố

$$f(x) = a_0 x^n + a_1 x^{n-1} + \dots + a_n \equiv 0 \pmod{p} \quad (4)$$

với $n < p$, $a_0 \not\equiv 0 \pmod{p}$, *có không quá n nghiệm.*

Chứng minh. Chúng ta chứng minh định lý này bằng phương pháp phản chứng. Giả sử trái lại rằng phương trình (4) có ít nhất $n + 1$ nghiệm khác nhau là

$$x \equiv x_0, x_1, \dots, x_n \pmod{p}.$$

Khi ấy vì x_1 nghiệm đúng phương trình (4) nên ta có đồng dư thức $f(x_1) \equiv 0 \pmod{p}$.

Chia đa thức $f(x)$ cho đa thức $x - x_1$, giả sử ta được
$$f(x) = (x - x_1) f_1(x) + r_1,$$
trong đó $f_1(x)$ là đa thức bậc $n - 1$ với hệ số nguyên, với hệ số của x^{n-1} là a_0 và $r_1 = f(x_1) \equiv 0 \pmod p$. Chính vì vậy phương trình (4) tương đương với phương trình :
$$(x - x_1) f_1(x) \equiv 0 \pmod p. \quad (5)$$
Từ giả thiết x_2 nghiệm đúng phương trình (4) ta có đồng dư thức
$$(x_2 - x_1) f_1(x_2) \equiv 0 \pmod p.$$
Nhưng $x_2 - x_1 \not\equiv 0 \pmod p$ và p là một số nguyên tố nên từ đồng dư thức trên ta suy ra
$$f_1(x_2) \equiv 0 \pmod p.$$
Chia đa thức $f_1(x)$ cho đa thức $x - x_2$ giả sử ta được
$$f_1(x) = (x - x_2) f_2(x) + r_2,$$
trong đó $f_2(x)$ là đa thức bậc $n - 2$ với hệ số nguyên và hệ số của x^{n-2} là a_0 và $r_2 = f_1(x_2) \equiv 0 \pmod p$. Từ đây vì $r_2 \equiv 0 \pmod p$ phương trình (5) và do đó cả phương trình (4) tương đương với phương trình
$$(x - x_1)(x - x_2) f_2(x) \equiv 0 \pmod p.$$
Cứ tiếp tục lý luận như vậy sau n bước ta được phương trình
$$(x - x_1)(x - x_2) \ldots (x - x_n) f_n(x) \equiv 0 \pmod p)$$
tương đương với phương trình (4). Nhưng $f_n(x)$ là đa thức bậc không mà hệ số của số hạng bậc cao nhất là a_0 nên $f_n(x) = a_0$ và vì vậy phương trình (4) tương đương với phương trình
$$a_0(x - x_1)(x - x_2) \ldots (x - x_n) \equiv 0 \pmod p. \quad (6)$$
Theo giả thiết $x \equiv x_0 \pmod p$ là nghiệm của phương trình (4) nên nó cũng là nghiệm của phương trình (6), nghĩa là ta có đồng dư thức
$$a_0(x_0 - x_1)(x_0 - x_2) \ldots (x_0 - x_n) \equiv 0 \pmod p$$
Từ đồng dư thức này với $x_0 - x_i \not\equiv 0 \pmod p$, $i = 1, 2, \ldots, n$ và p là số nguyên tố ta suy ra $a_0 \equiv 0 \pmod p$ là

điều mâu thuẫn với giả thiết. Đến đây định lý được chứng minh.

Chú ý. a. Nếu phương trình

$$f(x) = a_0x^n + a_1x^{n-1} + \dots + a_n \equiv 0 \pmod{p} \qquad (7)$$

với $n < p$ và p là số nguyên tố, có quá n nghiệm thì các hệ số của nó đều là bội của p.

Thật vậy, từ giả thiết và lặp lại cách chứng minh định lý trên ta có $a_0 \equiv 0 \pmod{p}$ nên phương trình (7) tương đương với phương trình

$$a_1x^{n-1} + a_2x^{n-2} + \dots + a_n \equiv 0 \pmod{p}.$$

Phương trình này có nhiều hơn n nghiệm. Lại theo cách lập luận trên ta sẽ có $a_1 \equiv 0 \pmod{p}$.

Cứ tiếp tục lý luận như thế cuối cùng ta được tất cả các hệ số $a_0, a_1, \dots, a_n$ đều là bội của p.

b. Về mặt thực hành, qua chứng minh định lý ở trên ta suy ra rằng nếu ta biết một nghiệm nào đó của phương trình (4) thì ta có thể chuyển việc giải phương trình (4) về việc giải một phương trình đồng dư có bậc nhỏ hơn.

Ví dụ. Giải phương trình đồng dư

$$f(x) = x^5 + x^4 + x^3 + x^2 - 2x + 9 \equiv 0 \pmod{11}.$$

Ta có $f(1) = 11 \equiv 0 \pmod{11}$; chia $f(x)$ cho $x - 1$, ta được thương $f_1(x) = x^4 + 2x^3 + 3x^2 + 4x + 2$ và dư $r_1 = 11 \equiv 0 \pmod{11}$. Phương trình đã cho tương đương với phương trình, $(x-1)(x^4+2x^3+3x^2+4x+2) \equiv 0 \pmod{11}$.

Xét phương trình

$$f_1(x) = x^4+2x^3+3x^2+4x+2 \equiv 0 \pmod{11}.$$

Ta thấy rằng $f_1(-1) = 0 \equiv 0 \pmod{11}$; chia $f_1(x)$ cho $x+1$ ta được thương $f_2(x) = x^3 + x^2 + 2x + 2$ và dư $r_2 = 0 \equiv 0 \pmod{11}$.

Xét phương trình

$$f_2(x) = x^3+x^2+2x+2 \equiv 0 \pmod{11}.$$

Ta lại thấy $f_2(-1) = 0 \equiv 0 \pmod{11}$, chia $f_2(x)$ cho $x+1$ ta được thương $f_3(x) = x^2+2$ và dư $r_3 = 0 \equiv 0 \pmod{11}$. Phương trình $f_3(x) = x^2 + 2 \equiv 0 \pmod{11}$ nghiệm đúng với $x=3$ và $x=-3$ nhưng $3 \not\equiv -3 \pmod{11}$ và phương trình theo môđun nguyên tố nên $x \equiv 3 \pmod{11}$ và $x \equiv -3 \pmod{11}$ là hai nghiệm duy nhất của nó.

Vậy phương trình đã cho tương đương với phương trình $(x-1)(x+1)^2(x-3)(x+3) \equiv 0 \pmod{11}$ và nó có bốn nghiệm là

$$x \equiv \pm 1, \pm 3 \pmod{11}.$$

3. Định lý Vinsơn. *Nếu p là một số nguyên tố thì ta có đồng dư thức*

$$(p-1)! + 1 \equiv 0 \pmod{p}.$$

Chứng minh. Định lý là hiển nhiên với $p = 2$, vì vậy để chứng minh ta có thể giả sử $p > 2$. Ta hãy xét phương trình đồng dư

$$(x-1)(x-2)\dots(x-p+1) - (x^{p-1}-1) \equiv 0 \pmod{p}.$$

Phương trình này có không ít hơn $p-1$ nghiệm đôi một khác nhau và vế trái của nó là một đa thức bậc nhỏ hơn $p-1$, vì vậy theo chú ý ở trên tất cả các hệ số của đa thức đó đều là bội của p và nói riêng hệ số tự do cũng là bội của p. Hệ số tự do đó là

$$(-1)(-2)\dots(-(p-1)) + 1 = (p-1)! + 1,$$

cho nên ta được

$$(p-1)! + 1 \equiv 0 \pmod{p}.$$

Định lý Vinsơn cho ta *điều kiện cần* để một số tự nhiên $p > 1$ là số nguyên tố, song điều kiện đó cũng là *điều kiện đủ*. Thật vậy, nếu $p = p_1 d$, $1 < d < p$ thì $(p-1)! \equiv 0 \pmod{d}$ bởi vậy $(p-1)! + 1 \not\equiv 0 \pmod{d}$. Nhưng vì $p \equiv 0 \pmod{d}$ nên nếu $(p-1)!+1 \not\equiv 0 \pmod{d}$ thì cũng có $(p-1)! + 1 \not\equiv 0 \pmod{p}$. Nói khác đi nếu $(p-1)! + 1 \equiv 0 \pmod{p}$ thì số tự nhiên $p > 1$ sẽ là một số nguyên tố.

BÀI TẬP

7.1. Giải các phương trình

a) $7x \equiv 25 \pmod{117}$; b) $67x \equiv 61 \pmod{183}$; c) $213x \equiv 137 \pmod{2113}$; d) $1296x \equiv 1105 \pmod{2113}$; e) $(a + b)x \equiv a^2 + b^2 \pmod{ab}$, với $(a, b) = 1$.

7.2. Giải các phương trình

a) $6x \equiv 27 \pmod{33}$; b) $186x \equiv 374 \pmod{422}$; c) $129x \equiv 321 \pmod{471}$; d) $285x \equiv 177 \pmod{924}$; e) $(a + 1)x \equiv a^2 - 1 \pmod{m}$.

7.3. Cho p là một số nguyên tố và a là một số nguyên dương nhỏ hơn p. Chứng minh rằng phương trình

$$ax \equiv b \pmod{p}$$

có nghiệm là

$$x \equiv b(-1)^{a-1} \frac{(p-1)(p-2)\dots(p-a+1)}{a!} \pmod{p}.$$

Áp dụng giải các phương trình

a) $10x \equiv 21 \pmod{89}$; b) $14x \equiv 81 \pmod{211}$.

7.4. Cho $m_1, m_2, \dots, m_k$ là những số nguyên dương đôi một nguyên tố cùng nhau. Đặt $m = m_1 . m_2 \dots m_k$, $M_i = \frac{m}{m_i}$ $(i = 1, 2, \dots, k)$. Giả sử M_i' là số nguyên thỏa mãn $M_i M_i' \equiv 1 \pmod{m_i}$ $(i = 1, 2, \dots, k)$. Chứng minh rằng hệ phương trình

$$\begin{cases} x \equiv b_1 \pmod{m_1}, \\ x \equiv b_2 \pmod{m_2}, \\ \dots\dots\dots \\ x \equiv b_k \pmod{m_k} \end{cases}$$

có nghiệm là

$$x \equiv M_1 M_1' b_1 + M_2 M_2' b_2 + \dots + M_k M_k' b_k \pmod{m}.$$

Áp dụng giải các hệ phương trình

a) $\begin{cases} x \equiv 1 \pmod{3}, \\ x \equiv 4 \pmod{5}, \\ x \equiv 2 \pmod{7}, \\ x \equiv 9 \pmod{11}, \\ x \equiv 3 \pmod{13}; \end{cases}$ b) $\begin{cases} x \equiv a \pmod{3}, \\ x \equiv b \pmod{5}, \\ x \equiv c \pmod{7}. \end{cases}$

7.5. Giải các hệ phương trình

a) $\begin{cases} x \equiv 4 \pmod{5}, \\ x \equiv 1 \pmod{12}, \\ x \equiv 7 \pmod{14}; \end{cases}$ b) $\begin{cases} x \equiv 13 \pmod{14}, \\ x \equiv 6 \pmod{35}, \\ x \equiv 26 \pmod{45}; \end{cases}$

c) $\begin{cases} 5x \equiv 1 \pmod{12}, \\ 5x \equiv 2 \pmod{8}, \\ 7x \equiv 3 \pmod{11}; \end{cases}$ d) $\begin{cases} 3x \equiv 1 \pmod{10}, \\ 4x \equiv 3 \pmod{5}, \\ 2x \equiv 7 \pmod{9}. \end{cases}$

7.6 Giải các hệ phương trình

a) $\begin{cases} x \equiv a \pmod{6}, \\ x \equiv 1 \pmod{8}; \end{cases}$ b) $\begin{cases} x \equiv 5 \pmod{8}, \\ x \equiv 8 \pmod{21}, \\ x \equiv a \pmod{35}, \end{cases}$

trong đó a là một số nguyên.

7.7. Hãy xác định a để các hệ phương trình sau đây có nghiệm

a) $\begin{cases} x \equiv 3 \pmod{11} \\ x \equiv 11 \pmod{20}, \\ x \equiv 1 \pmod{15}, \\ x \equiv a \pmod{18}; \end{cases}$ b) $\begin{cases} 2x \equiv a \pmod{3}, \\ 3x \equiv 1 \pmod{10}. \end{cases}$

7.8. Tìm tất cả các số tự nhiên $\leqslant 1000$ mà khi chia chúng cho 3, 5, 9, 11 ta được các số dư lần lượt là 1, 3, 4, 9.

7.9. Tìm số tự nhiên nhỏ nhất thỏa mãn các điều kiện: khi chia nó cho 7 dư 3, bình phương của số đó khi chia cho 7^2 dư 44, lập phương của số đó khi chia cho 7^3 dư 111.

7.10. a) Tìm các số nguyên mà khi chia nó cho số tự nhiên lẻ $m > 1$ dư là 1 và bình phương của số phải tìm chia cho m^2 dư $m + 1$.

b) Tìm các số nguyên mà khi chia nó cho số tự nhiên lẻ $m > 1$ dư là $m - 1$ và bình phương của số phải tìm chia cho m^2 dư 1.

7.11. Cho phương trình

$a_0x^n + a_1x^{n-1} + \ldots + a_n \equiv 0 \pmod{m}$ với $(a_0, m) = 1$.

Chứng minh rằng bao giờ cũng có thể đưa phương trình đã cho về dạng

$x^n + b_1x^{n-1} + \ldots + b_n \equiv 0 \pmod{m}$.

Áp dụng vào phương trình

$4x^3 - 8x - 13 \equiv 0 \pmod{27}$

7.12. Cho phương trình

$x^n + a_1x^{n-1} + ... + a_n \equiv 0 \pmod{m}$ với $(m, n) = 1$.

Chứng minh rằng bao giờ cũng tìm được số nguyên a để bằng phép đổi biến số $x = y + a$ ta đưa phương trình đã cho về phương trình

$$y^n + b_2y^{n-2} + ... + b_n \equiv 0 \pmod{m},$$

trong đó không có số hạng bậc $n - 1$.

Áp dụng vào phương trình

$$x^3 + 5x^2 + 6x - 8 \equiv 0 \pmod{13}.$$

7.13. Cho p là một số nguyên tố và n là một số nguyên dương. Giả sử khi chia n cho p ta được thương là q và dư là r. Chứng minh rằng với mọi số nguyên x_0 đều có

$$x_0^n \equiv x_0^{q+r} \pmod{p}.$$

Từ đó hãy nêu lên một qui tắc làm giảm bậc của phương trình có bậc chưa nhỏ hơn p.

Áp dụng vào phương trình

$$x^{101} + 3x^{15} + x^{11} - 3x^5 + 9x^2 + 10x - 5 \equiv 0 \pmod{11}.$$

7.14. Giải các phương trình

a) $x^2 + 2 \equiv 0 \pmod{19}$; b) $5x^2 + x + 4 \equiv 0 \pmod{13}$;

c) $x^3 + x^2 - x + 16 \equiv 0 \pmod{17}$; d) $x^4 - 3x^2 - 11 \equiv 0$ (mod [illegible])

7.15. Giải các phương trình

a) $x^3 + 1 \equiv 0 \pmod{25}$; b) $x^3 + 2x + 9 \equiv 0 \pmod{19}$;

c) $2x^2 - x - 1 \equiv 0 \pmod{27}$; d) $7x^4 + 19x + 25 \equiv 0 \pmod{27}$.

7.16. Giải các phương trình

a) $3x^3 + 4x^2 - 7x - 6 \equiv 0 \pmod{15}$; b) $(x^2 + 1)(x^2 + 3) \equiv 0 \pmod{35}$;

c) $6x^3 - 3x^2 - 13x - 10 \equiv 0 \pmod{30}$;

d) $2x^{16} - 17x^{15} + 13x^8 - 3x^5 + 12x + 5 \equiv 0 \pmod{20}$.

7.17. Giải các phương trình nguyên

a) $x^2 + 19y + 2 = 0$; b) $x^3 + 1 = 25y$; c) $2x^3 - 5x^2 + 4x + 15y + 11 = 0$; d) $x^2 - 20y + 3 = 0$.

7.18. Cho phương trình đồng dư theo môđun nguyên tố p

$f(x) = x^n + a_1x^{n-1} + ... + a_n \equiv 0 \pmod{p}$ với $0 < n < p$.

Chứng minh rằng phương trình đã cho có đủ n nghiệm khi và chỉ khi đa thức dư trong phép chia $x^p - x$ cho $f(x)$ có tất cả các hệ số đều là bội của p.

7.19. Giả sử p là một số nguyên tố lẻ, n là một số tự nhiên lớn hơn 1 chia hết p − 1 và a là một số nguyên nguyên tố với p. Chứng minh rằng phương trình

$$x^n \equiv a \pmod{p}$$

có nghiệm khi và chỉ khi

$$a^{\frac{p-1}{n}} \equiv 1 \pmod{p}$$

và khi có nghiệm thì nó có n nghiệm.

7.20. Cho p là một số nguyên tố lẻ, a là một số nguyên nguyên tố với p. Chứng minh rằng

a) Phương trình $x^2 \equiv a \pmod{p}$ có nghiệm khi và chỉ khi

$$a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$$

và khi có nghiệm thì nó có hai nghiệm.

b) Phương trình $x^2 \equiv a \pmod{p}$ vô nghiệm thì

$$a^{\frac{p-1}{2}} \equiv -1 \pmod{p}.$$

7.21. Cho phương trình

$$ax^2 + bx + c \equiv 0 \pmod{p}$$

với p là một số nguyên tố lẻ và a là một số nguyên nguyên tố với p. Chứng minh rằng

a) Nếu $b^2 \equiv 4ac \pmod{p}$ thì phương trình đã cho có đúng một nghiệm.

b) Nếu $b^2 \not\equiv 4ac \pmod{p}$ thì phương trình đã cho có nghiệm khi và chỉ khi

$$(b^2 - 4ac)^{\frac{p-1}{2}} \equiv 1 \pmod{p}.$$

7.22. Cho p là một số nguyên tố lẻ. Chứng minh rằng phương trình $x^2 + 1 \equiv 0 \pmod{p}$ có nghiệm khi và chỉ khi $p \equiv 1 \pmod{4}$.

7.23. Sử dụng kết quả bài tập trên chứng minh rằng có vô số số nguyên tố dạng 4k + 1.

7.24. a) Cho p là một số nguyên tố và x, x' là các số nguyên thỏa mãn $xx' \equiv 1 \pmod{p}$. Chứng minh rằng nếu x chạy qua một hệ thặng dư thu gọn môđun p thì x' cũng chạy qua một hệ thặng dư thu gọn môđun p.

b) Chứng minh định lý Lépnit: Nếu p là một số tự nhiên lớn hơn 1 thì p là nguyên tố khi và chỉ khi ta có đồng dư thức

$$(p-2)! - 1 \equiv 0 \pmod{p}.$$

c) Từ định lý Lépnit hãy suy ra định lý Vinsơn.

7.25. Cho $p = 4k+1$ là một số nguyên tố. Chứng minh rằng phương trình $x^2 + 1 \equiv 0 \pmod{p}$ có nghiệm là $x \equiv \pm (2k)! \pmod{p}$.

Áp dụng giải các phương trình nguyên:

a) $x^2 + 13y + 1 = 0$; b) $x^2 - 17y + 1 = 0$.



TRẢ LỜI CHỈ DẪN HOẶC CÁCH GIẢI CÁC BÀI TẬP

1.1 *Trả lời*: a) $b = 28, 29, 30$ tương ứng $r = 27, 16, 5$. b) vô nghiệm.

Chỉ dẫn. Hãy sử dụng hệ thức $bq \leqslant a < b(q+1)$.

1.2. Ta có $(k^n - b^n) - (k^n - a) = a - b^n$ chia hết cho $k - b$, bởi vậy bằng cách chọn k sao cho $|k - b| > a - b^n$ ta sẽ được $a = b^n$.

1.3. *Chỉ dẫn.* Hãy sử dụng nguyên tắc ngăn kéo Điriclê.

1.4. *Chỉ dẫn.* Hãy sử dụng kết quả câu b) bài 1.3.

a) $m^3 + 11m = m(m^2 - 1) + 12m$;

b) $m^5 - m = m(m^2 - 1)(m^2 - 4) + 5m(m^2 - 1)$;

c) $m^5 - 5m^3 + 4m = m(m^2 - 1)(m^2 - 4)$ và $120 = 3.5.8$;

d) $3m^4 - 14m^3 + 21m^2 - 10m = 5m(m^2 - 1)(m - 2) - 8m(m - 1)(m - 2)$ và $24 = 3.8$.

1.5. Hai khả năng có thể xảy ra

1) Trong năm số đã cho có ba số khi chia cho 3 có cùng một số dư, khi ấy tổng của ba số này chia hết cho 3.

2) Trường hợp còn lại là có ba số nào đó khi chia cho 3, không có cùng dư, khi ấy ba số này có tổng chia hết cho 3.

1.6. Giả sử $x = 3a + r$, $y = 3b + s$, $-1 \leqslant r, s \leqslant 1$.

Khi ấy $x^2 + y^2 = 3(3a^2 + 3b^2 + 2ar + 2bs) + r^2 + s^2$ chia hết cho 3

Suy ra rằng $r^2 + s^2$ chia hết cho 3, nhưng $0 \leqslant r^2 + s^2 < 3$ nên $r^2 + s^2 = 0$, nghĩa là phải có $r = 0$ và $s = 0$.

1.7. *Chỉ dẫn.* $1^3 + 2^3 + ... + n^3 = \frac{n^2(n+1)^2}{4}$;

$$1^5 + 2^5 + ... + n^5 = \frac{n^2(n+1)^2(2n^2+2n-1)}{12}.$$

1.8. *Chỉ dẫn.* Với số tự nhiên lẻ k ta có $a^k + b^k \,\vdots\, a + b$.

Các tổng $1^k + n^k$, $2^k + (n-1)^k$, ... đều chia hết cho $n+1$; các tổng $1^k + (n-1)^k$, $2^k + (n-2)^k$, ... đều chia hết cho n và vì :

$$(n, n+1) = 1 ; 1 + 2 + ... + n = \frac{n(n+1)}{2}$$

1.9. a) *Chỉ dẫn.* $11^{10} - 1 = 10(11^9 + 11^8 + ... + 11 + 1)$

b) Ta có $2222^{5555} + 5555^{2222} = (2222^{5555} + 4^{5555}) + (5555^{2222} - 4^{2222}) - (4^{5555} - 4^{2222})$. Trong đó $2222^{5555} + 4^{5555} \,\vdots\, 2222 + 4\ (= 7.318)$; $4^{5555} - 4^{2222} = 4^{2222} \times (4^{3333} - 1) = 4^{2222}(64^{1111} - 1) \,\vdots\, 63$; $5555^{2222} - 4^{2222} \,\vdots\, 5555 - 4\ (= 7.783)$.

1.10. a) Gọi $A_n = 16^n - 15n - 1$, bằng phép qui nạp theo n ta có $A_1 = 0 \,\vdots\, 225$; giả sử $A_n \,\vdots\, 225$ khi ấy ta có $A_{n+1} = 16^{n+1} - 15(n+1) - 1 = 16.16^n - 15n - 16 = 16^n - 15n - 1 + 15(16^n - 1) = A_n + 15(16^n - 1) \,\vdots\, 225$.

Cách thứ hai. Ta có $A_n = (15+1)^n - 15n - 1 = 15^n + n \cdot 15^{n-1} + ... + \frac{n(n-1)}{2}15^2 + n \cdot 15 + 1 - 15n - 1$

chia hết cho 225.

b) *Chỉ dẫn* $3^{2^{4n+1}} + 2 = 3^{2(15+1)^n} + 2 = 3^{5t+2} + 2 =$
$= 9(3^5)^t + 2 = 9\ (22 . 11 + 1)^t + 2$ chia hết cho 11.

c) Ta có $5^{2n-1} . 2^{n+1} + 3^{n+1} . 2^{2n-1} = (19 + 1) . 50^{n-1} + (19 - 1) . 12^{n-1} = 19\ (50^{n-1} + 12^{n-1}) + (50^{n-1} - 12^{n-1})$, trong đó $50^{n-1} + 12^{n-1} \vdots 2 ; 50^{n-1} - 12^{n-1} \vdots 50 - 12 (=38)$.

1.11. Giả sử $a + b = nt$, $t \in Z$. khi ấy $a^n + b^n = a^n + (nt - a)^n = n^n t^n - C_n^1 n^{n-1} t^{n-1} a + ... + n^2 a^{n-1} t$

bởi vì n là số lẻ. Từ đó suy ra $a^n + b^n \vdots n^2$.

1.12 a) *Chỉ dẫn. Cách thứ nhất* : qui nạp theo n.
Cách thứ hai : khai triển $(n + 1)^n$.

Chỉ dẫn. Hãy vận dụng kết quả câu a) bằng cách đặt $2^n - 1 = m$.

1.13. Qui nạp theo n. Với $n = 1$ ta có $A_n = k^2 - 1 \vdots 8$ bởi vì $k^2 - 1 = (k + 1)(k - 1)$ là tích của hai số chẵn liên tiếp (do k là số lẻ) mà hai số chẵn liên tiếp ắt có một số chia hết cho 2 một số chia hết cho 4. Giả sử đã có $A_n \vdots 2^{n+2}$, nghĩa là $A_n = k^{2^n} - 1 = 2^{n+2}.t$. Khi ấy $k^{2^{n+1}} = k^{2^n}.2 = (2^{n+2}t + 1)^2 = 2^{2n+4}t^2 + 2^{n+3}t + 1 = 2^{n+3}(2^{n+1}t^2 + t) + 1 = 2^{n+3} q + 1$. Từ đó ta có $A_{n+1} = k^{2^{n+1}} - 1 = 2^{n+3} q$ chia hết cho 2^{n+3}.

1.14. a) Giả sử $n = 3q + r, r = 0, 1, 2$. Khi ấy dễ dàng suy ra rằng $2^n - 1$ chia hết cho 7 khi $r = 0$.

b) Với $r = 0, 1, 2$ ta đều có $2^n + 1 = 7t + 2^r + 1$ không chia hết cho 7.

1.15. a) Điều kiện để một số chia hết cho 72 là nó chia hết đồng thời cho 8 và 9. $3^n + 63 \vdots 9$ khi và chỉ khi $n \geqslant 2$. Mặt khác $3^n + 63 = 3^n - 1 + 8^2 \vdots 8$ khi và chỉ khi $3^n - 1 \vdots 8$ tức là khi và chỉ khi n là số chẵn
Trả lời : $n = 2k, k \geqslant 1$.

b) Giả sử $n = 10t + r$ $(0 \leqslant r < 9)$. Ta có điều kiện để $n^{10} + 1 \vdots 10$ là $r^{10} + 1 \vdots 10$. Xét $r = 0, 1, ..., 9$ ta được $3^{10} + 1 \vdots 10$; $7^{10} + 1 \vdots 10$. Vậy $n = 10t + 3$ hoặc $n = 10t + 7$.

Trả lời : $n = 10t \pm 3$, $t \in Z$, $n \geqslant 0$.

c) Ta có $323 = 17.19$. Gọi $A = 20^n + 16^n - 3^n - 1$. Với $n = 2k$ ta có $16^{2k} - 1 \vdots 16^2 - 1$ $(= 15.17)$ nên $A \vdots 17$; lại có $16^{2k} - 3^{2k} \vdots 16^2 - 3^2$ $(= 13.19)$ nên $A \vdots 19$; từ đó $A \vdots 323$. Với $n = 2k + 1$ ta có $16^{2k} - 1 \vdots 17$ nên 16^{2k+1} chia cho 17 có dư là 16 nên A không chia hết cho 17.

Trả lời : $n = 2k$, $k \in Z$.

1.16. Ta có $a_n - b_n = 2^{n+2}$ không chia hết cho 5 nên a_n và b_n không đồng thời chia hết cho 5. Mặt khác $a_n b_n = (2^{2n+1} + 1)^2 - 2^{2(n+1)} = 2^{2(2n+1)} + 1 = 4^{2n+1} + 1 \vdots 5$ nên a_n và b_n có ít nhất một số chia hết cho 5.

Cách thứ hai. Giả sử $n = 4k + r$, $r = 0, 1, 2, 3$

$r = 0$ có $a_n \vdots 5$, b_n chia cho 5 dư 1;

$r = 1$ có $b_n \vdots 5$, a_n chia cho 5 dư 3;

$r = 2$ có $b_n \vdots 5$, a_n chia cho 5 dư 1;

$r = 3$ có $a_n \vdots 5$, b_n chia cho 5 dư 3.

1.17. a) Giả sử k là số nguyên lớn nhất sao cho $2^k \leqslant n$ và P là tích của tất cả các số lẻ không vượt quá n.

Số $2^{k-1}.P.A$ biểu diễn tổng tất cả các số hạng, ngoài số hạng $2^{k-1}.P\frac{1}{2^k}$, ta có tổng này là nguyên suy ra A không nguyên.

b) Giả sử k là số nguyên lớn nhất với điều kiện $3^k \leqslant 2n+1$ và P là tích tất cả các số nguyên tố cùng nhau với 6, không vượt quá $2n+1$. Số $3^{k-1}.P.B$. biểu thị tổng tất cả các số hạng, ngoài số hạng $3^{k-1}.P.\frac{1}{3^k}$, tổng này là nguyên, từ đó suy ra B không nguyên.

1.18. a) Giả sử $ax - by = 1$, $x, y \in \mathbf{Z}$. Từ giả thiết $a > 1$, $b > 1$ ta có $x \neq 0$, $y \neq 0$ và b không chia hết x, a không chia hết y. Giả sử $y = aq + \beta$, $0 < \beta < a$. Đặt $\alpha = x - bq$ ta có $a\alpha - b\beta = 1$ và $0 < \alpha < b$ vì $a > 1$ và $b > 1$. Tính duy nhất của cặp α, β được suy từ $(a, b) = 1$.

b) Giả sử $ax - by = k$, $x = bq + \alpha$, $0 \leqslant \alpha < b$. Đặt $\beta = y - aq$ ta có $a\alpha - b\beta = k$ và $-1 < \beta < a$ bởi vì $1 < a < b$, $1 < k \leqslant b$ Tính duy nhất của cặp α, β được suy từ $(a, b) = 1$.

1.19. *Chỉ dẫn: Cách thứ nhất.* Hãy chứng minh rằng tập hợp các ước chung là trùng nhau.

Cách thứ hai. a) Dựa vao nhân xét $(xy + z, y) = (z, y)$.

1.20. a) *Chỉ dẫn:* Dựa vao thuật toán Ơclid.

b) $n^4 + 3n^2 + 1 = n(n^3 + 2n) + n^2 + 1$, $n^3 + 2n = n(n^2 + 1) + n$, $n^2 + 1 = n \cdot n + 1$.

c) $m^2n + 2m = m(mn + 1) + m$, $mn + 1 = m \cdot n + 1$

1.21. a) Đặt $(a, b) = d$, $a = da_1$, $b = db_1$, $(a_1, b_1) = 1$ $(a \leqslant b)$. Chuyển về tìm a_1 và b_1: $a_1 + b_1 = 12$, $(a_1, b_1) = 1$ $a_1, b_1 > 1$. *Trả lời:* $a = 36$, $b = 396$ hoặc $a = 180$, $b = 252$.

b) *Trả lời.* Với $a \leqslant b$ ta có $a = 20$, $b = 420$ hoặc $a = 60$, $b = 142$.

c) *Trả lời.* $a = 315$, $b = 495$.

d) Giả sử $a = 24a_1$, $b = 24b_1$, $(a_1, b_1) = 1$, $a_1 \leqslant b_1$. Khi ấy từ $[a, b]\,(a, b) = ab$ ta có $a_1b_1 = 104 = 1.104 = 8.13$. Suy ra từ đó rằng $a_1 = 1$, $b_1 = 104$ hoặc $a_1 = 8$, $b_1 = 13$.

Trả lời : a = 24, b = 2496 hoặc a = 192, b = 312.

1.22. Giả sử $n = rn_1$, $a = ra_1$, $(a_1, n_1) = 1$. Ta có $(n, ab) = (rn_1, ra_1b) = r(n_1, a_1b) = r(n_1, b)$ (vì $(a_1, n_1) = 1$)

— Vì $n_1 \mid n$ nên $(n_1, b) \mid (n, b) = s$ do đó $(n, ab) = r(n_1, b) \mid rs$ suy ra $(n, ab) \mid (n, rs)$.

— Mặt khác $r \mid a$, $s \mid b$ nên $(n, rs) \mid (n, ab)$. Vậy $(n, rs) = (n, ab)$.

1.23. $(a, b, c) = ((a, b), c) = (a, r_1, c) = ((a, c), r_1) = (a, r_2, r_1)$ $(1248, 1784, 2730) = (1248, 536, 234) = (234, 78, 78) = 78$.

1.24. Chứng minh tập hợp các ước chung trùng nhau. Giả sử :

$$\delta \Big| \left(\frac{a+b}{2}, \frac{b+c}{2}, \frac{c+a}{2}\right) \text{ thế thì } \delta \Big| \frac{a+b}{2} + \frac{a+c}{2} - \frac{b+c}{2}$$

tức là $\delta \mid a$; tương tự có $\delta \mid b$, $\delta \mid c$.

Ngược lại, giả sử $\delta \mid (a, b, c)$ thế thì $\delta \mid a+b$ và $2 \mid a+b$ (vì a, b là những số lẻ, δ là một số lẻ), từ đó

$\delta \Big| \frac{a+b}{2}$; tương tự $\delta \Big| \frac{b+c}{2}$, $\delta \Big| \frac{c+a}{2}$

Trả lời : (2365, 2205, 4851) = 21.

1.25. *a) Cách thứ nhất.* Giả sử

$$\begin{aligned} m &= nq + r_1 \\ n &= r_1q_1 + r_2 \\ &\dots\dots \\ r_{k-2} &= r_{k-1}q_{k-1} + r_k, \\ r_{k-1} &= r_kq_k, \end{aligned}$$

tức là $(m, n) = r_k$. Phải chứng minh rằng $(a^m - 1, a^n - 1) = a^{r_k} - 1$. Ta có :

$$a^m - 1 = (a^n - 1)(a^{m-n} + a^{m-2n} + \dots + a^{r_1}) + a^{r_1} - 1.$$

Bởi vậy $(a^m - 1, a^n - 1) = (a^n - 1, a^{r_1} - 1)$. Lại vì $a^n - 1 =$
$= (a^{r_1} - 1)\ (a^{n-r_1} + a^{n-2r_1} + ... + a^{r_2}) + a^{r_2} - 1$ nên
$(a^n - 1, a^{r_1} - 1) = (a^{r_1} - 1, a^{r_2} - 1)$, bởi vậy $(a^m - 1, a^n - 1) =$
$= (a^{r_1} - 1, a^{r_2} - 1)$. Cứ tiếp tục như vậy cuối cùng ta được
$(a^m - 1, a^n - 1) = (a^{r_{k-1}} - 1, a^{r_k} - 1) = a^{r_k} - 1$ (vì $a^{r_k} - 1$ là ước của $a^{r_{k-1}} - 1$), do r_k là ước của r_{k-1}).

Cách thứ hai. Gọi $(a^n - 1, a^r - 1) = d$, $(m, n) = \delta$ ta có $a^{\delta} - 1 \mid (a^m - 1, a^n - 1) = d$ (vì $\delta \mid m$, $\delta \mid n$). Ngược lại giả sử $\delta = mx_0 - ny_0$ với x_0, y_0 là những số nguyên dương, ta có $d \mid a^{mx_0} - 1 - (a^{ny_0} - 1)$ nên $d \mid a^{ny_0} \times$
$\times (a^{mx_0 - ny_0} - 1)$ tức là $d \mid a^{yn_0}(a^{\delta} - 1)$. Nhưng $(a, d) = 1$ nên $(a^{ny_0}, d) = 1$ từ đó $d \mid a^{\delta} - 1$. Vậy $a^{\delta} - 1 = d$.

b) Gọi $d = \left(\dfrac{a^m - 1}{a - 1}, a - 1\right)$, $\delta = (m, a - 1)$. Ta có

$\dfrac{a^m - 1}{a - 1} = a^{m-1} + a^{m-2} + ... + a + 1 = (a^{m-1} - 1) +$
$+ (a^{m-2} - 1) + ... + (a - 1) + m = (a - 1)t + m$ (bởi vì $a - 1 \mid a^k - 1$ với $k = 1, 2, ..., m - 1$). Do đó

$$d = \left(\frac{a^m - 1}{a - 1}, a - 1\right) = ((a-1)t + m, a - 1) = (m, a - 1) = \delta.$$

c) Gọi $d = (a! + 1, (a + 1)! + 1)$ thì ta có $d \mid (a + 1)(a! + 1) =$
$= (a + 1)! + (a + 1)$ cho nên $d \mid (a + 1)! + (a + 1) - (a + 1)! - 1$, nghĩa là $d \mid a$.

Từ $d \mid a$ ta có $d \mid a!$, do đó $d \mid (a! + 1) - a!$ hay $d \mid 1$. Vậy $d = 1$.

1.26. a) Ta có $C_n^k = \dfrac{n!}{(n-k)!\,k!}$ và $C_{n-1}^{k-1} =$

$$= \frac{(n-1)!}{(n-k)!\,(k-1)!}$$

cho nên

$$k\,C_n^k = n\,C_{m-1}^{k-1} \quad (\bigstar)$$

Từ đẳng thức ($\bigstar$) suy ra $n \mid k.\,C_n^k$, nhưng $(n, k) = 1$ cho nên $n \mid C_n^k$.

b) Áp dụng công thức ($\bigstar$) ở câu a) ta có

$$(m+n)\,C_{m+n-1}^{n-1} = n\;C_{m+n}^{n}$$

cho nên suy ra $n \mid (m+n)\,C_{m+n-1}^{n-1}$. (Song $(m+n, n) = (m, n) = 1$ nên $n \mid C_{m+n-1}^{n-1}$. Ta thấy rằng $C_{m+n-1}^{n-1} = \dfrac{(m+n-1)!}{m!(n-1)!}$ bởi vậy từ $n \mid C_{m+n-1}^{n-1}$ ta suy ra $m!\,n! \mid (m+n-1)!$.

1.27. Đặt $Q = a^n + b^n$, $S_o = a^m + b^m$, $S_k = a^{m-nk} + (-1)^k b^{m-nk}$, ta sẽ có $S_{k-1} = Qa^{m-nk} - S_k b^n$ (**) $(k = 1, 2, ..)$. Thật vậy bằng cách đặt ta có $Q.a^{m-nk} - S_k b^n = (a^n + b^n)\,a^{m-nk} - b^n(a^{m-nk} + (-1)^k b^{m-nk}) =$

$$= a^{n+m-nk} + (-1)^{k-1} b^{n+m-nk} = a^{m-n(k-1)} + (-1)^{k-1} b^{m-n(k-1)} = S_{k-1}.$$

Bây giờ giả sử $m = np + r$, $0 \leqslant r < p$. Ta thấy rằng nếu $S_o b \vdots Q$ thì $S_1 b^n = Qa^{m-n} - S_o \vdots Q$. Nhưng $(b^n, Q) = (b^n, a^n + b^n) = (b^n, a^n) = 1$ (vì $(a, b) = 1$) nên $S_1 \vdots Q$. Vậy nếu $S_o \vdots Q$ (theo giả thiết) thì $S_1 \vdots Q$ và lại từ công thức (**) từ $S_1 \vdots Q$ có $S_2 \vdots Q$,... cứ như vậy $S_p \vdots Q$. Nhưng $S_p = a^{m-pn} + (-1)^p b^{m-np} = a^r + (-1)^p b^r$ ta có

$|S_p| \leqslant a^r + b^r < Q$ mà $S_p \vdots Q$ nên buộc $S_p = 0$, điều này kéo theo p là số lẻ. $S_p = a^r - b^r = 0$ cho ta $a^r = b^r$, nhưng a, b > 1 ta phải có r = 0 do đó m = np nghĩa là $m \vdots n$.

1.28. Giả sử (a, c) = d ta có $a = a_1 d$, $c = c_1 d$, $(a_1, c_1) = 1$. Từ đó ta có $a_1 b = d^{n-1} c_1^n$. Nhưng $(d, b) \mid (a, b)$ mà (a, b) = 1 nên (d, b) = 1 và do đó $(d^{n-1}, b) = 1$. Ở trên ta đã có $b \mid d^{n-1} c_1^n$ nên $b \mid c_1^n$. Từ $(a_1, c_1) = 1$ ta có $(a_1, c_1^n) = 1$. Song đã có $c_1^n \mid a_1 b$ nên $c_1^n \mid b$. Vậy $b = c_1^n$ và ta đặt $\alpha = d$, $\beta = c_1$.

1.29. Chứng minh bằng phép qui nạp toán học. Giả sử có k số đôi một nguyên tố cùng nhau $a_1 = 2^{n_1} - 3$, $a_2 = 2^{n_2} - 3, \ldots, a_k = 2^{n_k} - 3$, trong đó $2 = n_1 < n_2 < \ldots < n_k$. Ta hãy tìm số $a_{k+1} = 2^{n_{k+1}} - 3$ nguyên tố với tất cả k số a_i ở trên (i = 1, 2,..., k). Đặt $l = a_1 a_2 \ldots a_k$, thế thì trong $l + 1$ số $2^0, 2^1, \ldots, 2^l$ ắt có hai số khi chia cho l ta có cùng số dư. Giả sử hai số đó là 2^r và $2^s (r > s)$. Như vậy l là ước của $2^r - 2^s = 2^s(2^{r-s} - 1)$. Nhưng $(l, 2) = 1$ nên $l \mid 2^{r-s}$, chẳng hạn $2^{r-s} - 1 = lt$. Ta hãy lấy $a_{k+1} = 2^{r-s+2} - 3 = 4lt + 1 > a_k$ mà $(a_{k+1}, l) = 1$ nên a_{k+1} nguyên tố với $a_1, a_2, \ldots, a_k$. Nếu cứ quá trình ấy mà tiến hành thì ta tìm được vô số các số dạng $2^n - 3$ đôi một nguyên tố cùng nhau.

1.30. Bằng phép qui nạp toán học ta có thể chứng minh được công thức:

$$U_{m+n} = U_{m-1} U_n + U_m U_{n+1} \qquad (*)$$

(chẳng hạn qui nạp theo n).

a) Giả sử $(U_n, U_{n+1}) = d$. Ta có $U_{n+1} = U_{n-1} + U_n$ cho nên $(U_{n+1}, U_n) = (U_{n-1}, U_n) = d$. Tiếp tục ta có $d = (U_1, U_2) = 1$

b) Giả sử m > n. Áp dụng thuật toán Ơclid trên

hai số m và n ta có chẳng hạn $m = nq_0 + r_1$, $n = r_1q_1 + r_2$, ..., $r_{k-2} = r_{k-1}q_{k-1} + r_k$, $r_{k-1} = r_kq_k$, nghĩa là $r_k = (m, n)$. Từ đó $(U_m, U_n) = (U_{nq_0+r_1}, U_n)$ và dựa vào công thức (*) ta được $(U_m, U_n) = (U_{nq_0-1}U_{r_1} + U_{nq_0}U_{r_1+1}, U_n)$. Song $U_{nq_0} \vdots U_n$ (hãy chứng minh) nên $(U_m, U_n) = (U_{nq_0-1}U_{r_1}, U_n)$. Lại vì $(U_{nq_0-1}, U_n) = 1$ nên ta được $(U_m, U_n) = (U_{r_1}, U_n)$. Tiếp tục lập luận này sẽ cho ta $(U_n, U_{r_1}) = (U_{r_1}, U_{r_2})$ và vì vậy $(U_m, U_n) = (U_n, U_{r_1}) = (U_{r_1}, U_{r_2}) = ... = U_{r_k} = U_{(m,n)}$.

c) Giả sử n/m, chẳng hạn $m = nk$. Ta chứng minh U_n . U_{nk} bằng phép qui nạp theo k. Với $k = 1$, $n = m$ ta có $U_m = U_n$ nên $U_n | U_m$. Giả sử $U_n | U_{nk}$, $k \geq 1$, ta chứng minh rằng $U_n | U_{n(k+1)}$. Ta có $U_{n(k+1)} = U_{nk+n}$ và áp dụng hệ thức (*) ta có $U_{n(k+1)} = U_{nk-1}U_n + U_{nk}U_{n+1}$ nên $U_n | U_{n(k+1)}$. Ngược lại giả sử U_n/U_m thế thì $(U_n, U_m) = U_n$ mà theo câu b) $(U_m, U_n) = U_{(m, n)}$ ta được $(m, n) = n$, bởi vậy $n | m$.

d) *Chỉ dẫn*: Áp dụng câu b) ta chỉ cần xét dãy các số nguyên tố sánh đôi. Muốn vậy dãy chỉ số có thể chẳng hạn là dãy các số nguyên tố (xem bài thứ hai) 2, 3, 5 7, 11, 13, ...

1.31. *Chỉ dẫn*: Bằng phương pháp qui nạp, chứng minh như bài 1.29.

a) Giả sử đã có k số đôi một nguyên tố cùng nhau $t_1 = 1$ $t_2 = 3$, ..., t_k. Đặt $a = t_1t_2... t_k$ thì ta có số trong dãy đang xét

$$t_{k+1} = (a + 1)(2a + 1) = \frac{1}{2}(2a + 1)(2a + 2).$$

Rõ ràng $t_{k+1} > t_k$. Hơn nữa $(a + 1, a) = 1$, $(2a + 1, a) = 1$ nên $(t_{k+1}, a) = 1$ do đó t_{k+1} nguyên tố với tất cả $t_1, t_2, ..., t_k$,

b) Giả sử có k số đôi một nguyên tố cùng nhau $T_1 = 1$, $T_2 = 4$, ..., T_k. Đặt $a = T_1 . T_2 \dots T_k$ ta có số

$$T_{k+1} = (2a+1)(3a+1)(6a+1) = \frac{1}{6}(6a+3)(6a+2)(6a+1)$$

lớn hơn T_k và T_{k+1} nguyên tố với a nên T_{k+1} nguyên tố với tất cả $T_1, T_2, \dots, T_k$.

1.32. Giả sử $[a, a+1, a+2] = m$, ta có $m = [a(a+1), a+2]$ nên hoặc $m = a(a+1)(a+2)$ nếu a là số lẻ hoặc $m = \frac{1}{2}a(a+1)(a+2)$ nếu a là số chẵn, bởi vì $(a(a+1), a+2)$ hoặc bằng 1 hoặc bằng 2 tùy theo a là số lẻ hoặc số chẵn.

1.33. a) Trước hết ta có: $(a, b, c)\left(\frac{b}{(a, b)}, \frac{c}{(a, c)}\right) =$

$$= \left(\frac{b}{(a, b)}(a, b, c), \frac{c}{(a, c)}(a, b, c)\right) = \left(\frac{b}{(a, b)}((a, b), (b, c)),\right.$$

$$\left.\frac{c}{(a, c)}((a, c), (b, c))\right) = \left(\left(b, \frac{b(b, c)}{(a, b)}\right), \left(c, \frac{c(b, c)}{(a, c)}\right)\right) =$$

$$= \left((b, c), \frac{b(b, c)}{(a, b)}, \frac{c(b, c)}{(a, c)}\right) = (b, c)\left(1, \frac{b}{(a, b)}, \frac{c}{(a, c)}\right) =$$

$= (b, c)$. Suy ra từ đó rằng

$$\frac{(b, c)}{(a, b, c)} = \left(\frac{b}{(a, b)}, \frac{c}{(a, c)}\right).$$

$$\frac{(b, c)[a, (b, c)]}{a(b, c)} = \left(\frac{[a, b]}{a}, \frac{[a, c]}{a}\right)$$

tức là $[a, (b, c)] = ([a, b], [a, c])$.

b) Áp dụng kết quả câu a) ta có

$$[(a, b), (a, c)] = ([(a, b), a], [(a, b), c]) =$$

$$= (a, [(a, b), c]) = (a, ([a, c], [b, c])) =$$

$$= ((c, [a, c]), [b, c]) = (a, [b, c]).$$

1.34. a) $\dfrac{abc}{[a, b, c]} = \dfrac{(a, b)\,[a, b]\,c}{[a, b, c]} = (a, b)\ ([a, b], c) =$

$$= (a, b)\ [(a, c), (b, c)] = \frac{(a, b)\,(a, c)\,(b, c)}{((a, c), (b, c))} =$$

$$= \frac{(a, b)\,(b, c)\,(c, a)}{(a, b, c)}.$$

b) Suy ra từ kết quả câu a).

1.35. Đặt $(a_1, a_2, \ldots, a_n) = d$, $[a_1, a_2, \ldots, a_n] = m$

$(A_1, A_2, \ldots, A_n) = D$, $[A_1, A_2, \ldots, A_n] = M$.

a) Ta có $\left(\dfrac{M}{A_1}, \dfrac{M}{A_2}, \ldots, \dfrac{M}{A_n}\right) = 1$. Bởi vì

$a_i = \dfrac{A}{A_i} = \dfrac{A}{M} \cdot \dfrac{M}{A_i}$ $(i = 1, 2, \ldots, n)$ cho nên ta có

$$d = \left(\frac{A}{M} \cdot \frac{M}{A_1}, \frac{A}{M} \cdot \frac{M}{A_2}, \ldots, \frac{A}{M} \cdot \frac{M}{A_n}\right) =$$

$$= \frac{A}{M}\left(\frac{M}{A_1}, \frac{M}{A_2}, \ldots, \frac{M}{A_n}\right) = \frac{A}{M}.$$

Từ đó ta được $d.\,M = A$.

b) Giả sử $\dfrac{A}{D} = x$, ta phải chứng minh $x = m$.

Ta có $x = a_1 \dfrac{A_1}{D} = a_2 \dfrac{A_2}{D} = \ldots = a_n \dfrac{A_n}{D} \left(= \dfrac{A}{D}\right)$ nên

$a_i | x$ với mọi $i = 1, 2, \ldots, n$. Từ đó $m | x$ nghĩa là $x = mq$, $q \geqslant 1$. Bởi vì $\dfrac{A_i}{D} = \dfrac{x}{a_i} = \dfrac{m}{a_i} q$, $i = 1, 2, \ldots, n$ nên

$q \left| \left(\dfrac{A_1}{D}, \dfrac{A_2}{D}, \ldots, \dfrac{A_n}{D}\right)\right.$. mà $\left(\dfrac{A_1}{D}, \dfrac{A_2}{D}, \ldots, \dfrac{A_n}{D}\right) = 1$

vì thế $q = 1$, nói khác đi ta được $x = m$.

∴

2.1 a) $n^4 + 4 = (n^2 + 2n + 2)(n^2 - 2n + 2)$, trong đó ta có $n^2 + 2n + 2 > 5$, $n^2 - 2n + 2 > 1$.

b) $n^4 + n^2 + 1 = (n^2 + n + 1)(n^2 - n + 1)$.

c) Nếu $n = 2k$ thì $n^4 + 4^n$ là số chẵn lớn hơn 2.

Nếu $n = 2k + 1$ thì $n^4 + 4^n = n^4 + 4(2^k)^4 =$

$$= (n^2 + 2^{2k+1} + n.2^{k+1})(n^2 + 2^{2k+1} - n.2^{k+1}).$$

2.2 Đáp số $n = 5$. Thật vậy $1^4 + 2^4 = 17$, $2^4 + 3^4 = 97$, $3^4 + 4^4 = 337$, $4^4 + 5^4 = 881$ là những số nguyên tố $5^4 + 6^4 = 1921 = 17.113$ là hợp số.

2.3 a) $A_n = 3.2^{2^{2n}} + 1 > 7$ và $A_n \vdots 7$. Thật vậy bởi vì $A_n = 6(2^{4^n - 1} - 1)$ mà $2^{4^n - 1} - 1 \vdots 2^3 - 1$.

b) $B_n = 2^{2^{n+1}} + 2^{2^n} + 1 > 21$ và $B_n \vdots 21$ Thật vậy, $B_2 = 273 = 21.13$. Giả sử $B_n \vdots 21$ ta có $B_{n+1} \vdots 21$, bởi vì $B_{n+1} - B_n = 2^{2^{n+2}} - 2^{2^n} = 2^{2^n}(8^{2^n} - 1) = 2^{2^n} \times$ $\times (64^{2^{n-1}} - 1)$

mà $64^{2^{n-1}} - 1 \vdots 64 - 1$. Vậy $\frac{1}{3} B_n \vdots 7$ và $\frac{1}{3} B_n > 7$.

c) $C_n = 2^{4n+2} + 1 = (2^{2n+1} + 2^{n+1} + 1)(2^{2n+1} - 2^{n+1} + 1)$.

Ta nhận thấy $5 = 2^2 + 1 \mid 2^{4n+2} + 1$ bởi vậy $C_n \vdots 5$. Lại có $2^{2n+1} + 2^{n+1} + 1 > 2^{2n+1} - 2^{n+1} + 1 = 2^{n+1} \times$ $\times (2^n - 1) + 1 > 2^3 3 + 1$ (vì $n > 1$), nghĩa là $2^{m+1} +$ $+ 2^{n+1} + 1 > 2^{2n+1} - 2^{n+1} + 1 > 25$. Vậy $C_n = (2^{2n+1} +$ $+ 2^{n+1} + 1)(2^{2n+1} - 2^{n+1} + 1)$ gồm hai nhân tử > 25 và có ít nhất một nhân tử chia hết cho 5, nói khác đi $\frac{1}{5} C_n$ là hợp số.

Chú ý : Có thể dựa vào bài tập 1.16 để chứng minh $\frac{1}{5} C_n$ là hợp số.

2.4. a) Giả sử p là một nguyên tố. Chia p cho 30 ta được chẳng hạn $p = 30t + r$, $t, r \in \mathbf{N}$, $0 < r < 30$. Nếu r là hợp số thì r có ước nguyên tố $q \leqslant \sqrt{30}$ tức là $q \leqslant 5$, nghĩa là chỉ có thể $q = 2, 3, 5$. Nhưng với $q = 2$,

3, 5 đều có p chia hết cho 2, 3, 5 suy ra p là hợp số, trái với giả thiết p là nguyên tố. Vậy $r = 1$ hoặc r là một số nguyên tố. Khi chia số nguyên tố cho 60 thì kết quả trên không còn đúng vì chẳng hạn 109 là số nguyên tố, ta có $109 = 60 + 49$.

b) Với $p = 30t + r$ là một số nguyên tố lớn hơn 5 thì r chỉ có thể là 1, 7, 11, 13, 17, 19, 23, 29 cho nên $p^2 = 30s + 1$ (với $r = 1, 11, 19, 29$ hoặc $p^2 = 30s + 19$ (với $r = 7, 13, 17, 23$). Từ đó $p^4 = 30k + 1$, $k \in N$. Vậy nếu $p_1, p_2, \ldots, p_n$ là những số nguyên tố lớn hơn 5 mà $p_1^4 + p_2^4 + \ldots + p_n^4 = q$ là một số nguyên tố thì $q = 30u + n$, $u \in N$ và từ đó buộc là $(n, 30) = 1$ vì nếu trái lại thì q không phải là nguyên tố.

2.5. Từ $2p+1 = n^3$, $n \in N$ ta có n phải là số lẻ $\geqslant 3$. $2p = n^3 - 1 = (n-1)(n^2+n+1)$. Vì $n-1$ là số chẵn $\geqslant 2$ nên $n-1 = 2$. Từ $n = 3$ ta suy ra $p = 13$ là số nguyên tố và $2.13+1 = 27 = 3^3$. *Đáp số :* $p = 13$.

2.6. p phải là số nguyên tố lẻ và từ đó $p = r + 2 = s - 2$. Ta suy ra r, $p = r+2$, $s = p+2 = r+4$ là ba số nguyên tố lẻ liên tiếp. Vậy $r = 3$, $p = 5$, $s = 7$.

Đáp số : $p = 5$.

2.7. Giả sử $1+p+p^2+p^3+p^4 = n^2$. Khi ấy dễ thấy $(2p^2+p)^2 < (2n)^2 < (2p^2+p+2)^2$ nên $(2n)^2 = (2p^2+p+1)^2$ Từ đó ta có $p^2 - 2p - 3 = 0$ nên $p = 3$, Nhưng với $p=3$ ta có $1+3+3^2+3^3+3^4 = 11^2$ nên có đáp số $p = 3$.

2.8. Từ $1+p = n^s$ ta có $p = n^s - 1 = (n-1)(n^{s-1} + n^{s-2} + \ldots + 1)$ cho nên $n-1 = 1$, $n = 2$. Vậy $p = 2^s - 1$, $2 \leqslant s \leqslant 10$. Nhưng nếu $p = 2^s - 1$ là nguyên tố thì s phải là nguyên tố (bài tập 2.23) nên $s = 2, 3, 5, 7$. Với $s = 2$ có $p = 3$; $s = 3$ có $p = 7$; $s = 5$ có $p = 31$; $s = 7$ có $p = 127$ là những số nguyên tố.

Đáp số : $p = 3, 7, 31, 127$

2.9. Rõ ràng với $k > 1$ các số $m = 2^k - 2$ và $n = 2^k \times (2^k - 2)$ có cùng các ước nguyên tố và với chúng $m + 1 = 2^k - 1$ và $n + 1 = (2^k - 1)^2$ cũng có cùng các ước nguyên tố.

2.10. Ta biết rằng nếu p là ước nguyên tố của $m!$ thì p phải là ước của một nhân tử nào đó của tích $m! = 1. 2... m$, nghĩa là ắt có $1 < a \leqslant m$ sao cho $p \mid a$. Vậy nếu $n \mid (n-1)!$ và $n+2 \mid (n-1)!$ thì n và $n+2$ không phải là những số nguyên tố.

-- Đảo lại, giả sử n không chia hết $(n-1)!$ và $n+2$ không chia hết $(n-1)!$. Khi ấy từ n không chia hết $(n-1)!$ với $n > 1$ ta có hoặc $n = 4$ hoặc n là nguyên tố. Thật vậy giả sử n không phải là nguyên tố thì $n = ab$ với $2 \leqslant a, b \leqslant n - 1$. Nếu $a \neq b$ thì a và b là hai nhân tử trong tích $(n-1)!$, khi ấy $n \mid (n-1)!$ là vô lý. Vậy $a = b \geqslant 2$. Nhưng nếu $a = b > 2$ thì ta có $2a < (a-1)(a+1) = a^2 - 1 = n - 1$, hơn nữa $a < 2a$ thành thử $a.2a \mid (n-1)!$ tức là $a.2a = 2a^2 = 2n \mid (n-1)!$ kéo theo $n \mid (n-1)!$ (vì n là số lẻ) là vô lý. Từ đó $a = b = 2$ và ta được $n = 4$.

Như vậy hoặc $n = 4$ hoặc n phải là một số nguyên tố, nhưng $n = 4$ thì $n + 2 = 6 \mid (n-1)!$ trái với ở trên nên n là nguyên tố.

Đồng thời $n+2$ cũng là nguyên tố. Thật vậy nếu như $n+2 = ab$, $3 \leqslant a \leqslant b$ thì $b \leqslant \frac{n+2}{3} \leqslant \frac{n-1}{2}$. Nhưng nếu $a \neq b$ thì $n + 2 = ab \mid (n-1)!$ là trái với ở trên; còn nữa nếu $a = b$ thì $2(n+2) = 2a^2 = a(2a) \mid (n-1)!$ cũng trái với ở trên (lưu ý $(2, n+2) = 1$ nên $n+2 \mid (n-1)!$). Vậy $n+2$ là nguyên tố.

2.11. Với mỗi số tự nhiên n, ta gọi q_n là số nguyên tố lớn nhất thỏa mãn $q_n \leqslant 6n+1$ và p_n là số nguyên tố đứng liền sau q_n thì $p_n \geqslant 6n + 5$ nên $p_n - q_n \geqslant 4$. Với $n = 1$ có $q_1 = 7$, $p_1 = 11$, lấy $m = p_n$ ta có cặp q_m, p_m.

Tiếp tục như thế, thì do tập hợp các số nguyên tố là vô hạn ta có vô hạn cặp q_m, p_m là cặp các số nguyên tố không phải sinh đôi.

2.12. a) Nếu $p > 3$ thì p^2 chia cho 3 có dư là 1 do đó $8p^2 + 1$ chia hết cho 3. Bởi vậy suy ra $p = 2, 3$. Nếu $p = 2$ ta có $8p^2 + 2p + 1 = 37$ là nguyên tố. Nếu $p = 3$ ta có $8p^2 + 2p + 1 = 79$ là nguyên tố. *Đáp số* $p = 2; 3$.

b) Xét thấy $4p(4p + 1)(4p + 2) = 8p(4p + 1)(2p + 1)$ chia hết cho 3 và $8p(2p + 1)$ không chia hết cho 3 vậy $4p + 1$ là số lớn hơn 3 chia hết cho 3.

2.13. Giả sử $m > 2$, khi ấy $a = m! - 1 > 1$ nên a có ít nhất một ước nguyên tố p, dĩ nhiên $p \leqslant m! - 1$ tức là $p < m!$. Mặt khác $p > m$ vì nếu $p \leqslant m$ thì $p \mid m!$, do đó $p \mid 1$ là vô lý.

2.14. Ta có trong năm số p, $p + 6 = p + 1 + 5$, $p + 8 = p + 3 + 5$, $p + 12 = p + 2 + 10$, $p + 14 = p + 4 + 10$ có ít nhất một số chia hết cho 5, nhưng ngoài p ra bốn số còn lại đều lớn hơn 5 bởi vậy $p = 5$. Với $p = 5$ ta có $p + 6 = 11$, $p + 8 = 13$, $p + 12 = 17$, $p + 14 = 19$ đều là những số nguyên tố. *Đáp số* $p = 5$

2.15. a) $(4m + 1)(4n + 1) = 4(4mn + m + n) + 1$.

Giả sử cho trước r số nguyên tố dạng $4m + 1$ là p_1, $p_2, \ldots, p_r$ chẳng hạn. Khi ấy xét số $a = 4p_1 . p_2 \ldots p_n - 1$ đây là một số dạng $4m + 3$ lớn hơn 1 cho nên a có ước nguyên tố. Rõ ràng ước nguyên tố đó không thể là 2 vì nếu vậy, ước nguyên tố này sẽ là ước của 1. Hơn nữa không phải mọi ước nguyên tố của a đều có dạng $4m + 1$, vì nếu tất cả các ước nguyên tố của a đều có dạng $4m + 1$ thì a cũng phải có dạng ấy (nhưng a không có dạng $4m + 1$). Vậy a phải có ước nguyên tố p dạng $4m + 3$. Ta thấy $p \neq p_i$, với mọi $i = 1, 2, \ldots, r$, vì nếu $p = p_i$ nào đấy thì $p \mid 1$ là vô lý.

b) Giải tương tự như trên và xét số $a = 6p_1 p_2 \dots p_r - 1$ trong đó $p_1, p_2, \dots, p_r$ là những số nguyên tố dạng $6m+5$ cho trước. Ta có a có ước nguyên tố p dạng $6m+5$ và $p \neq p_i$, mọi $i = 1, 2, \dots, r$.

2.16. *Đáp số.* $p = 2 = \frac{2.3}{2} - 1$ và $p = 5 = \frac{3.4}{2} - 1$.

Chỉ dẫn. Với $n \geqslant 4$ ta có $\frac{n(n+1)}{2} - 1 =$

$= \frac{1}{2}(n-1)(n+2)$, trong đó $n-1$ và $n+2$ cùng lớn hơn 2 và một trong chúng có một số là chẵn.

2.17. *Đáp số:* $p = 2$, $p = 5$, $p = 11$.

Chỉ dẫn. Với $n \geqslant 4$ có $\frac{n(n+1(n+2)}{6} + 1 = \frac{(n+3)(n^2+2)}{6}$, trong đó $n+3 > 6$, $n^2+2 > 17$. Hơn nữa trong $n+3$ và n^2+2 có hoặc một số chẵn, một số chia hết cho 3 hoặc một trong chúng chia hết cho 6.

2.18. a) Không thể có vì nếu $p = 2$ thì $p+2d$ là hợp số, còn nếu p lẻ thì $p+d$ là hợp số.

b) Chẳng hạn p, $p + 2$, $p + 4$,... là một cấp số phải tìm thì p hoặc bằng 2 hoặc $p = 3k+r$, $r = 1, 2$. Nhưng trong ba số p, $p+2$, $p+4$ có một số chia hết cho 3 nên số ấy phải là p, vậy $p = 3$ với cấp số chỉ có ba số hạng. Với $p = 3$ ta có $p+2 = 5$, $p+4 = 7$ là những số nguyên tố. *Đáp số:* 3, 5, 7.

c) Xét p, $p+10$, $p+20$,... ta thấy trong ba số hạng liên tiếp ắt có một số chia hết cho 3 từ đó $p = 3$ và cấp số có ba số hạng. *Đáp số:* 3, 13, 23.

d) $p = 2$ thì $p+6 = 8$ là hợp số, $p = 3$ thì $p+6 = 9$ là hợp số. Vậy hoặc $p = 5$ hoặc $p = 5k+r$, $k \geqslant 1$, $r = 1, 2, 3, 4$. Với $r = 1, 2, 3, 4$ và $k > 1$ thì tương ứng $p+24$, $p+18$, $p+12$, $p+6$ là hợp số, cho nên nếu có, chỉ có thể $p = 5$. Với $p = 5$ ta có $p+6 = 11$, $p+12 = 17$, $p+18 = 23$,

$p+24 = 29$ là các số nguyên tố, $p+30 = 35$ là hợp số.

Trả lời. Cấp số phải tìm là 5, 11, 17, 23, 29.

2.19. Trong 3 số nguyên tố lẻ lớn hơn 3 phải có hai trong chúng cùng dạng $6k+1$ hoặc cùng dạng $6k+5$, bởi vậy hiệu của chúng là d hoặc 2d sẽ là bội của 6. Nghĩa là d là bội của 3, song vì d là chẵn nên d phải là bội của 6.

2.20. a) Xét dãy $k+1, k+2, \ldots, k+10$. (1)

Với $k = 1$ dãy (1) chứa 5 số nguyên tố.

Với $k = 0$, $k = 2$ dãy (1) chứa 4 số nguyên tố.

Với $k \geqslant 3$ thì dãy (1) có 5 số lẻ lớn hơn 3 mà trong ba số lẻ liên tiếp ắt có một số là bội của 3 nên dãy (1) lúc ấy chứa ít hơn 5 số nguyên tố. *Đáp số* $k = 1$.

b) Xét dãy $k + 1, k + 2, \ldots, k + 100$ (2)

Với $k = 1$ dãy (2) chứa 26 số nguyên tố, với $k = 0, 2, 3, 4$ dãy (2) chứa 25 số nguyên tố. Với $k \geqslant 5$ ta thấy dãy (2) chứa 50 số chẵn (đều là hợp số) và 50 số lẻ.

— Cứ 3 số lẻ (> 3) liên tiếp có một số bội của 3 nên trong 50 số lẻ ở trên có ít nhất 16 số là bội của 3.

— Hãy xem trong dãy (2) có bao nhiêu hợp số là bội của 5 mà không là bội của 2 và 3. Các số như vậy phải là $30t + r$, $0 \leqslant t \in Z$ và hoặc $r = 5$ hoặc $r = 25$. Ta lập tất cả các số dạng này theo dãy tăng vô hạn.

5, 25, 35, 55, 65, 85, 95, 115, 125, 145, 155,... (2') số hạng thứ n của dãy ký hiệu là U_n. Dễ dàng thấy rằng $U_{n+6} - U_n < 100$ với $n = 1, 2, \ldots$ Giả sử trong dãy U_1, $U_2, \ldots$ (2') có U_n là số hạng lớn nhất không vượt quá k. Khi ấy $U_n \leqslant k < U_{n+1} < U_{n+6} < U_n + 100 \leqslant k + 100$, từ đó thấy rằng trong dãy (2) có ít nhất 6 số trong dãy (2'), do đó có 6 số bội của 5 không là bội của 2 và 3.

— Hãy xem trong dãy (2) có ít nhất bao nhiêu số là bội của 7 mà không là bội của 2, 3 và 5. Các số này phải

có dạng $210q + r$, $0 \leqslant q \in Z$, $r = 7, 49, 77, 91, 119, 133, 161, 203$. Lập dãy số này.

7, 49, 77, 91, 119, 133, 161, 203, 217, 259, 287,... (2''). Số hạng thứ n của dãy ký hiệu là V_n. Dễ dàng thấy rằng $V_{n+3} - V_n < 100$ với n = 1, 2,... Giả sử V_n là số hạng lớn nhất của — (2'') không vượt quá k. Khi ấy ta có $V_n \leqslant k < V_{n+1} < V_{n+3} < V_n + 100 \leqslant k + 100$. Từ đó thấy rằng trong dãy (2) có ít nhất 3 số hạng trong dãy (2'') do đó trong (2) có ít nhất 3 số là bội của 7 mà đồng thời không là bội của 2, 3, 5 với $k \geqslant 7$.

Các lý luận ở trên cho ta thấy rằng với $k \geqslant 7$ thì dãy (2) chứa ít nhất $50 + 16 + 6 + 3 = 75$ hợp số và do đó dãy (2) chứa không hơn 25 số nguyên tố.

Với k = 5, k = 6 thì dãy (2) chứa các hợp số v_2, v_3, v_4 bởi vậy với $k > 1$ thì dãy (2) chứa không quá 25 số nguyên tố. *Trả lời*: k = 1.

2.21. Xét đa thức $f(x) = a_0x^n + a_1x^{n-1} + ... + a_n$, trong đó $a_0, a_1, ..., a_n$ là những số nguyên, $n \geqslant 1$, $a_0 \neq 0$. Hiển nhiên ắt có n_0 đủ lớn để $|f(n_0)| > 1$, bởi vậy $f(n_0)$ có ước nguyên tố p. Khi ấy hãy xét đẳng thức

$$f(n_0 + kp) = f(n_0) + k \cdot p \cdot f_1(n_0, p, k) \qquad (*)$$

với mọi k = 1, 2, 3,... ta có $f_1(n_0, p, k)$ là nguyên và cả ba số ở đẳng thức (*) đều chia hết cho p. Bởi vì với k đủ lớn ta có số $|f(n_0) + kp)|$ lớn hơn p và là bội của p nên nó là hợp số.

2.22. a) Giả sử trái lại có đa thức f(x) với hệ số nguyên mà $f(1) = 2$, $f(2) = 3$, $f(3) = 5$ thì đa thức $g(x) = f(x) - 2$ có nghiệm x = 1 nên $g(x) = (x - 1)\,h(x)$, h(x) là đa thức với hệ số nguyên. Từ đó $g(3) = 2h(3) = f(3) - 2 = 3$ là điều không thể xảy ra vì h(3) là một số nguyên.

b) Đặt $g_k(x) = (x-1)(x-2)\dots(x-k+1)(x-k-1)\dots(x-m)$, $k = 1, 2, \dots, m$. Ta có $g_k(k) \neq 0$, $g_k(a) = 0$ với $a \neq k$, $1 \leqslant a \leqslant m$. Khi ấy đa thức phải tìm là

$$f(x) = p_1 \frac{g_1(x)}{g_1(1)} + p_2 \frac{g_2(x)}{g_2(2)} + \dots + p_m \frac{g_m(x)}{g_m(m)}.$$

c) Đa thức phải tìm là

$$f(x) = x[(x-p_1)(x-p_2)\dots(x-p_m) + 1].$$

2.23. a) Giả sử trái lại $k > 0$ và $k \neq 2^n$ với mọi $n \in N$ thế thì $k = 2^m t$, $m \geqslant 0$, t là số lẻ > 1. Khi ấy $2^k + 1 = (2^{2^m})^t + 1$ chia hết cho $2^{2^m} + 1$ mà $2^k + 1 > 2^{2^m} + 1$ cho nên $2^k + 1$ là hợp số.

Chú ý: Ta có kết quả tổng quát hơn

— *Nếu $a^m + b^n$ là nguyên tố thì $(a, b) = 1$ và $(m, n) = 2^k$ với $k \geqslant 0$.* Thật vậy, giả sử $(m, n) = 2^t h$, $t \geqslant 0$, h là một số lẻ. Chẳng hạn $m = rh$, $n = sh$, thế thì nếu $h > 1$ sẽ có $a^m + b^n$ thực sự chia hết cho $a^r + b^s$, bởi vậy buộc $h = 1$. Mặt khác không thể $(a, b) > 1$ vì nếu $(a, b) = d > 1$ thì $a^m + b^n$ thực sự chia hết cho d, tức $a^m + b^n$ không phải là số nguyên tố.

— *Nếu $a^m + 1$ là nguyên tố thì hoặc $a = 1$ hoặc a là số chẵn và $m = 2^k$.* Thật vậy nếu a là số lẻ > 1 thì $a^m + 1$ là số chẵn lớn hơn 2. Còn nếu $m = 2^t h$, $t \geqslant 0$, h là số lẻ > 1 thì $a^m + 1$ có ước thực sự $a^{2^t} + 1$.

b) Nếu như k là hợp số thì $k = mt$, $1 < t < k$. Khi ấy $2^k - 1 = (2^t)^m - 1$ chia hết cho $2^t - 1$ và $1 < 2^t - 1 < 2^k - 1$, suy ra $2^k - 1$ là hợp số là điều mâu thuẫn.

Chú ý: Ta có kết quả tổng quát hơn.

Nếu $a^m - 1$ là nguyên tố thì $a = 2$ và m là nguyên tố. Thật vậy, với $a=1$ không được, với $a > 2$ thì $a^m - 1$ có ước thực sự là $a - 1$.

Nếu $a = 2$ mà $m = r.t$, $1 < r < m$ thì $2^m - 1$ có ước thực sự là $2^r - 1$. Vậy $a = 2$ và m là nguyên tố.

2.24. Nếu $2^n + 1$ và $2^n - 1$ cùng là những số nguyên tố thì n phải là số nguyên tố chẵn tức là $n = 2$. Trái với giả thiết $n > 2$. Hoặc có thể lý luận như sau: Bởi vì $(2^n, 3) = 1$ nên phải có $2^n = 3k \pm 1$, $k > 1$, từ đó $2^n \pm 1 = 3k$, $k > 1$, nghĩa là hoặc $2^n + 1$ có ước thực sự là 3 hoặc $2^n - 1$ có ước thực sự là 3.

2.25. Giả sử $m > n$ chẳng hạn $m = n + k, k > 0$, và giả sử $d = (F_m, F_n)$ dĩ nhiên ta có d là một số lẻ. Nếu đặt $x = 2^{2^n}$ thì chúng ta có:

$$\frac{F_{n+k} - 2}{F_n} = \frac{x^{2^k} - 1}{x + 1} = x^{2^k - 1} - x^{2^k - 2} + \dots - 1$$

cho nên $F_n \mid F_{n+k} - 2$. Từ đó $d \mid F_{n+k} - 2$, và vì $d \mid F_{n+k}$ ta có $d \mid 2$. Nhưng d là số lẻ nên $d = 1$.

Xét dãy $F_o, F_1, F_2, \dots$, vì chúng đều là những số lớn hơn 1 nên ta có dãy các ước nguyên tố tương ứng của chúng

$$p_o, p_1, p_2, \dots$$

dãy này đôi một phân biệt vì dãy

$$F_o, F_1, F_2, \dots$$

đôi một nguyên tố cùng nhau.

2.26. a) Ta có $-F_oF_1 \dots F_n = (1 - 2)(1 + 2)(1 + 2^2) \dots$

$$(1 + 2^{2^n}) = (1 - 2^2)(1 + 2^2) \dots (1 + 2^{2^n}) = \dots =$$

$= 1 - 2^{2^{n+1}} = 2 - F_{n+1}$ cho nên $F_{n+1} = 2 + F_oF_1 \dots F_n$.

b) Bằng qui nạp ta có với $n \geqslant 1$ thì $2^n \geqslant n + 1$, bởi vậy $2^{n+1} \mid 2^{2^n}$ cho nên $2^{2^{n+1}} - 1 \mid 2^{2^{2^n}} - 1$. Từ đó ta có $F_n \mid 2^{2^{2^n}} - 1$ (vì $2^{2^n} + 1 \mid 2^{2^{n+1}} - 1$) và bởi thế $F_n \mid 2^{2^{2^n}} - 1$. Nhưng $2^{2^{2^n}} - 1 \mid 2^{2^{2^n} + 1} - 2$ tức là $2^{2^{2^n}} - 1 \mid 2^{F_n} - 2$ nên ta có $F_n \mid 2^{F_n} - 2$.

Chú ý. Có thể sử dụng ngay câu a) với nhận xét rằng $2^{n+1} \mid 2^{2^n}$ và $F_n = 2^{2^{n+1}} - 1 = (2^{2^n} + 1)(2^{2^n} - 1)$.

— Đảo lại dễ thấy rằng *nếu số $m = 2^k + 1$ là ước của số $2^m - 2$ thì ta có m là số Phécma.*

2.27. Chẳng hạn $k = 6q - 1$, $q = 1, 2, \ldots$ Vì với mỗi số tự nhiên n ta thấy 2^{2^n} khi chia cho 3 dư 1, do đó số $2^{2^n} + k = 2^{2^n} - 1 + 6q$ lớn hơn 3 và là bội của 3, tức là tất cả các số $2^{2^n} - 1 + 6k$ là hợp số.

2.28. Giả sử $m > 1$ là một số tự nhiên và $n = m! + k$ $(k = 2, 3, \ldots, m)$. Ta có $k < m! + k$ và $k \mid m! + k$ bởi vậy $2^k - 1 < 2^{m!+k} - 1$ và $2^k - 1 \mid 2^{m!+k} - 1$, nghĩa là các số $2^{m!+k} - 1$ $(k = 2, 3, \ldots, m)$ đều là những hợp số. Như vậy ta có $m - 1$ hợp số Méexen liên tiếp, với m là số tùy ý.

2.29. Giả sử $n = 2k$, $k > 2$, ta có $M_n = 2^{2k} - 1 =$ $= (2^k + 1) \cdot (2^k - 1)$. Ta thấy rằng $2^k + 1 > 3$, $2^k - 1 > 3$ và vì trong ba số $2^k - 1$, 2^k, $2^k + 1$ có một số chia hết cho 3 mà $(2^k, 3) = 1$ nên hoặc $2^k - 1$ chia hết cho 3 hoặc $2^k + 1$ chia hết cho 3. Từ đó suy ra điều cần phải chứng minh.

2.30. Giả sử có vô số số tự nhiên n, với nó mỗi một trong các số n và $n + 1$ chỉ có một ước nguyên tố. Khi ấy coi $n > 8$ và có thể thấy rằng một trong các số n và $n + 1$ là chẵn số kia là lẻ, bởi vậy một số có dạng 2^h và số còn lại có dạng p^t với p là một số nguyên tố lẻ. Từ đó hoặc $2^h - 1 = p^t$ hoặc $2^h + 1 = p^t$. Nếu $p^t =$ $= 2^h - 1$ thì $t = 1$ và $2^h - 1 = p$ là số nguyên tố Mecxen. Nếu $p^t = 2^h + 1$ thì hoặc $t = 1$ khi đó $2^h + 1 = p$ là số nguyên tố Phecma; hoặc $t > 1$ thì khi đó $2^h = p^t -$ $1 = (p - 1)(p^{t-1} + p^{t-2} + \ldots + 1)$, $h > 1$, suy ra rằng t là số chẵn, chẳng hạn $t = 2k$ và như vậy $2^h = (p^k - 1) \times$ $\times (p^k + 1)$. Chính vì vậy các số $p^k - 1$, $p^k + 1$ khác với 2 cần phải là lũy thừa của 2. Với $p^k - 1 = 2$ ta có $p^k + 1 = 4$ suy ra $p = 3$, $2^h = 2.4 = 8$. Vậy ta đã chứng minh được

rằng nếu với $n > 8$ các số n và $n+1$ có chỉ một ước nguyên tố thì hoặc n là số nguyên tố Méexen hoặc $n+1$ là số nguyên tố Phécma.

— Ngược lại: Nếu $M_t = 2^t - 1$ là số nguyên tố Méc-xen thì các số M_t và $M_t + 1 = 2^m$ có chỉ một ước nguyên tố. Nếu $F_s = 2^{2^s} + 1$ là số nguyên tố Phécma thì mỗi một trong các số $F_s - 1 = 2^{2^s}$ và F_s có chỉ một ước nguyên tố.

∴

3.1. a) Giả sử $[-x] = \alpha$ ta có $\alpha < -x < \alpha + 1$ cho nên $-(\alpha + 1) < x < -\alpha$. Từ đó $[x] = -[-x] - 1$ hay là $[-x] = -[x] - 1$.

b) Giả sử $[x] = \alpha$, $[y] = \beta$, ta có $\alpha < x < \alpha + 1$ và $\beta < y < \beta + 1$ nên $\alpha + \beta < x + y < \alpha + \beta + 2$. Do $x + y = a$ là một số nguyên ta có $x + y = \alpha + \beta + 1$, tức là $a = \alpha + \beta + 1$. Từ đó $\alpha + \beta = a - 1$, nói khác đi $[x] + [y] = a - 1$.

3.2. a) Từ $[x] \leqslant x < [x] + 1$ ta có $[x] + m \leqslant x + m < [x] + m + 1$ mà $[x] + m$ là nguyên nên $[x + m] = [x] + m$.

b) Hãy xét với $n = 2k$ và $n = 2k+1$.

3.3. a) Gọi $\{x\} = \alpha$, $\{y\} = \beta$ ta có $[x] + [y] + \alpha + \beta = x + y$. Nếu $0 \leqslant \alpha + \beta < 1$ thì $[x+y] = [x] + [y]$; Nếu $1 \leqslant \alpha + \beta < 2$ thì $[x + y] = [x] + [y] + 1$.

b) Đặt $\{x_i\} = \alpha_i$, $i = 1, 2, \ldots, n$. Ta có

$$\left[\sum_{i=1}^{n} x_i\right] = \sum_{i=1}^{n} [x_i] + \left[\sum_{i=1}^{n} \alpha_i\right] \geqslant \sum_{i=1}^{n} [x_i].$$

Mặt khác vì $0 \leqslant \left[\sum_{i=1}^{n} \alpha_i\right] \leqslant n - 1$ cho nên

$$\sum_{i=1}^{n}[x_i] \leqslant \left[\sum_{i=1}^{n} x_i\right] \leqslant \sum_{i=1}^{n}[x_i] + n - 1.$$

c) Đặt $x = [x] + \alpha$, $y = [y] + \alpha$. $0 \leqslant \alpha, \beta < 1$. Hãy xét hai trường hợp $0 \leqslant \alpha + \beta < 1$ và $1 \leqslant \alpha + \beta < 2$.

3.4.a) Hãy chú ý $\left[\alpha + \frac{1}{2}\right] = [2\alpha] = \begin{cases} 0 \text{ nếu } 0 \leqslant \alpha < \frac{1}{2}, \\ 1 \text{ nếu } \frac{1}{2} \leqslant \alpha < 1. \end{cases}$

b) Đặt $\{x\} = \alpha$, ta có

$$[x] + \left[x + \frac{1}{2}\right] = 2[x] + \left[\alpha + \frac{1}{2}\right].$$

Mặt khác $2x = 2[x] + 2\alpha$ nên ta có $[2x] = 2[x] + [2\alpha]$. Dựa vào kết quả câu a) ta có điều cần phải chứng minh.

c) Giả sử $\alpha = \{x\}$, khi ấy ắt có số tự nhiên r sao cho

$$\frac{r}{n} \leqslant \alpha < \frac{r+1}{n}$$

với $0 \leqslant r < n$.

Vế trái của đẳng thức cần chứng minh : mỗi số hạng từ $[x]$ đến $\left[x + \frac{n-r-1}{n}\right]$ đều bằng $[x]$ vì số hạng lớn nhất trong chúng $x + \frac{n-r-1}{n} = [x] + \alpha + \frac{n-r-1}{n} < [x] + \frac{r+1}{n} + \frac{n-r-1}{n} = [x] + 1$, vậy tổng của chúng là $(n-r)[x]$. Tương tự lý luận như vậy ta thấy r số hạng còn lại, mỗi số hạng bằng $[x] + 1$ và tổng của chúng là $r([x] + 1)$. Như vậy vế trái là $n.[x] + r$. Mặt khác vế phải $[nx] = n[x] + [n\alpha] = n[x] + r$

3.5. a) *Cách thứ nhất.* Với x không nguyên ta có $[x] + [-x] = -1$ (bài tập 3. 1. a), bởi vậy từ $(m, n) = 1$ ta có $\frac{xm}{n}$ không nguyên $(1 \leqslant x \leqslant n-1)$ cho nên

$$\left[\frac{xm}{n}\right] + \left[\frac{(n-x)m}{n}\right] = \left[\frac{xm}{n}\right] + \left[\frac{-xm}{n}\right] + m = m - 1.$$

Nếu n là số lẻ thì vế trái có $\frac{n-1}{2}$ cặp như trên. Nếu n là số chẵn thì vế trái có $\frac{n-2}{2}$ cặp như trên và một số hạng $\left[\frac{m}{2}\right] = \frac{m-1}{2}$ (vì m phải lẻ), nên vế trái sẽ là $\frac{n-2}{2}(m-1) + \frac{m-1}{2} = (n-1)\frac{m-1}{2}$. Do đó trong mọi trường hợp vế trái đều là : $\frac{(m-1)(n-1)}{2}$.

Cách thứ hai. Xét đường thẳng $y = \frac{m}{n}x$ trong hệ tọa độ. Đề các vuông góc $[y] = \left[\frac{m}{n}x\right]$ là số các điểm nguyên nằm trên đường thẳng $x = k$ bị chắn giữa trục hoành và đường thẳng $y = \frac{m}{n}x$. Lưu ý một điều là với $1 \leqslant x \leqslant n-1$ trên đường thẳng $y = \frac{m}{n}x$ không có điểm nguyên. Ta có $S = \left[\frac{m}{n}\right] + \left[\frac{2m}{n}\right] + \dots + \left[\frac{(n-1)m}{n}\right]$ là số các điểm nguyên nằm « trong » tam giác tạo bởi đường thẳng $y = \frac{m}{n}x$, phần dương

của trục hoành và $x = n$. Ta có $2S$ là số các điểm nguyên nằm « trong » hình chữ nhật tạo bởi $y = m$, $x = n$ và hai bán trục. Với lưu ý ở trên ta có $2S = (m-1)(n-1)$; $S = \frac{(m-1)(n-1)}{2}$.

b) Số điểm nguyên trong hình chữ nhật

$$1 \leqslant x \leqslant p' \text{ và } 1 \leqslant y \leqslant q'$$

là $p'q'$.

Ta có p' số hạng đầu cho ta số điểm nguyên nằm ở phía dưới đường thẳng $y = \frac{q}{p} x$, trong hình chữ nhật nói trên ; q' số hạng sau cho ta số các điểm nguyên nằm ở phía trên đường thẳng $y = \frac{q}{p} x$, trong hình chữ nhật nói trên.

3. 6. Gọi $A = (\alpha + 1)(\alpha + 2) \ldots (p\alpha - 1) p\alpha$, ta có $A = \frac{(p\alpha)!}{\alpha!}$.

Ta phải chứng minh rằng số mũ của số nguyên tố p trong dạng phân tích tiêu chuẩn của A bằng α. Ta có số mũ của p trong dạng phân tích tiêu chuẩn của A được tính là hiệu của số mũ của p trong dạng phân tích tiêu chuẩn của $(p\alpha)!$ với số mũ của p trong dạng phân tích tiêu chuẩn của $\alpha!$ đó là :

$$\sum_{i \geqslant 1} \left[\frac{p\alpha}{p^i}\right] + \sum_{j \geqslant 1} \left[\frac{\alpha}{p^j}\right] = \alpha.$$

3. 7. Ta chú ý rằng với a, b, c là những số nguyên dương và $\sqrt{c}$ là vô tỷ thì bao giờ cũng có duy nhất hai số nguyên a_n, b_n sao cho

$$(a + b\sqrt{c})^n = a_n + b_n\sqrt{c},$$
$$(a - b\sqrt{c})^n = a_n - b_n\sqrt{c}$$

với n là một số nguyên dương cho trước.

a) Giả sử $(2+\sqrt{3})^n = a_n + b_n\sqrt{3}$.
Khi ấy ta có

$$(2+\sqrt{3})^n + (2-\sqrt{3})^n = a_n + b_n\sqrt{3} + a_n - b_n\sqrt{3} = 2a_n.$$

Bởi vì $0 < (2-\sqrt{3})^n < 1$, cho nên từ đẳng thức

$$(2+\sqrt{3})^n + (2-\sqrt{3})^n = 2a_n$$

ta có $\quad [(2+\sqrt{3})^n] = 2a_n - 1$

nghĩa là $\quad [(2+\sqrt{3})^n]$ là một số lẻ.

b) Giả sử $\quad (1+\sqrt{3})^n = a_n + b_n\sqrt{3}$

ta có $\quad (1+\sqrt{3})^n + (1-\sqrt{3})^n = 2a_n$.

Nếu $n = 2s$ là một số chẵn thì $0 < (1-\sqrt{3})^n < 1$ nên ta có

$$[(1+\sqrt{3})^n] = 2a_n - 1.$$

Nếu $n = 2s+1$ là một số lẻ thì $-1 < (1-\sqrt{3})^n < 0$ nên ta có :

$$[(1+\sqrt{3})^n] = 2a_n = (1+\sqrt{3})^n + (1-\sqrt{3})^n.$$

Nhưng $(1+\sqrt{3})^n + (1-\sqrt{3})^n = (1+\sqrt{3})^{2s+1} + (1-\sqrt{3})^{2s+1}$

$$= (1+\sqrt{3})^{2s}(1+\sqrt{3}) + (1-\sqrt{3})^{2s}(1-\sqrt{3}) =$$
$$= (4+2\sqrt{3})^s(1+\sqrt{3}) + (4-2\sqrt{3})^s(1-\sqrt{3}) =$$
$$= 2^s(2+\sqrt{3})^s(1+\sqrt{3}) + 2^s(2-\sqrt{3})^s(1-\sqrt{3}) =$$
$$= 2^s((2+\sqrt{3})^s + (2-\sqrt{3})^s + (2+\sqrt{3})^s - (2-\sqrt{3})^s\sqrt{3})).$$

Giả sử $(2+\sqrt{3})^s = a_s + b_s\sqrt{3}$, Khi ấy ta có

$$(1+\sqrt{3})^n + (1-\sqrt{3})^n = 2^s(2a_s + 6b_s) = 2^{s+1}(a_s + 3b_s).$$

Ta lại thấy rằng

$$(a_s + 3b_s)(a_s - 3b_s) = a_s^2 - 9b_s^2 = a_s^2 - 3b_s^2 - 6b_s^2 =$$
$$= (a_s + b_s\sqrt{3})(a_s - b_s\sqrt{3}) - 6b_s^2 = (2+\sqrt{3})^s(2-\sqrt{3})^s -$$
$$- 6b_s^2 = 1 - 6b_s^2 .$$

Nhưng $1 - 6b_s^2$ là một số lẻ nên $a_s + 3b_s$ là số lẻ, bởi

vậy ta có $[(1+\sqrt{3})^n] = 2a_n = 2^{s+1}(a_s + 3b_s)$ với $(a_s + 3b_s, 2) = 1$.

Tóm lại: số mũ cao nhất của 2 trong $[(1+\sqrt{3})^n]$ bằng 0 nếu n là số chẵn, bằng $s+1$ nếu $n = 2s+1$ là số lẻ.

3.8. Để chứng minh, hãy chứng tỏ rằng số mũ của số nguyên tố p trong sự phân tích tiêu chuẩn của tử số không nhỏ thua số mũ của số nguyên tố p trong sự phân tích tiêu chuẩn của mẫu số.

a) Trước hết ta thấy rằng với $a > 3$ ta có $\left[\frac{2n}{a}\right] \geqslant \left[\frac{n}{a}\right] + \left[\frac{n+2}{a}\right]$. Thật vậy giả sử $\frac{n}{a} = \alpha + x$, $\alpha = \left[\frac{n}{a}\right]$. Khi ấy nếu $0 \leqslant 2x < 1$ thì $\left[\frac{2n}{a}\right] = 2\alpha$ còn $\left[\frac{n+2}{a}\right] = \left[\frac{n}{a}\right] + \left[\frac{2}{a}\right] = \left[\frac{n}{a}\right] = \alpha$; nếu như $1 \leqslant 2x < 2$ thì $\left[\frac{2n}{a}\right] = 2\alpha + 1$, trong khi đó $\left[\frac{n+2}{a}\right] = \left[\frac{n}{a}\right] = \alpha$.

Vậy với số nguyên tố $p > 3$, số mũ của p trong phân tích tiêu chuẩn của $(2n)!$ không nhỏ hơn số mũ của p trong phân tích tiêu chuẩn của $n!\,(n+2)!$.

Với $a = 2$ ta xét hai trường hợp: $n = 2k$ ta có

$$\left[\frac{2n}{2}\right] = n = 2k, \left[\frac{n}{2}\right] + \left[\frac{n+2}{2}\right] = 2k + 1;$$

$n = 2k+1$ ta có $\left[\frac{2n}{2}\right] = n = 2k+1$, $\left[\frac{n}{2}\right] + \left[\frac{n+2}{2}\right] = 2k + 1$.

Vậy số mũ của 2 trong dạng phân tích tiêu chuẩn của $(2n)!$ trong trường hợp thứ nhất là 2k nên số mũ của 2

trong dạng phân tích tiêu chuẩn của tử số là $2k+1$, trong khi đó số mũ của 2 trong dạng phân tích tiêu chuẩn của mẫu số cũng bằng $2k+1$. Trong trường hợp thứ hai số mũ của 2 trong dạng phân tích tiêu chuẩn của tử số lớn hơn số mũ của 2 trong dạng phân tích tiêu chuẩn của mẫu số một đơn vị.

Với $a = 3$ ta xét ba trường hợp $n = 3k$, $n = 3k+1$, $n = 3k+2$. Với $n = 3k$ ta có:

$$\left[\frac{2n}{3}\right] = 2k = \left[\frac{n}{3}\right] + \left[\frac{n+2}{3}\right]; \text{ với } n = 3k+1$$

ta có $\left[\frac{2n}{3}\right] = 2k$, $\left[\frac{n}{3}\right] + \left[\frac{n+2}{3}\right] = 2k+1$;

với $n = 3k+2$ ta có $\left[\frac{2n}{3}\right] = \left[\frac{n}{3}\right] + \left[\frac{n+2}{3}\right] = 2k+1$.

Vậy trong cả ba trường hợp, số mũ của 3 trong dạng phân tích tiêu chuẩn của tử số không nhỏ hơn số mũ của 3 trong dạng phân tích tiêu chuẩn của mẫu số.

b) *Cách thứ nhất.* Ta đã biết $[2a] + [2b] \geqslant$ $\geqslant [a] + [b] + [a+b]$ (bài tập 3.3.c) cho nên

$$\left[\frac{2m}{p^i}\right] + \left[\frac{2n}{p^i}\right] \geqslant \left[\frac{m}{p^i}\right] + \left[\frac{n}{p^i}\right] + \left[\frac{m+n}{p^i}\right],$$

nghĩa là số mũ của số nguyên tố p trong dạng phân tích tiêu chuẩn của tử số không nhỏ hơn số mũ của p trong dạng phân tích tiêu chuẩn của mẫu số. Từ đó suy ra điều cần chứng minh.

Cách thứ hai. Đặt $f(m, n) = \dfrac{(2m)!\,(2n)!}{m!\,n!\,(m+n)!}$ ta kiểm tra thấy rằng $f(m+1, n) = nf(m, n) - f(m, n+1)$. Để chứng minh $f(m, n)$ là nguyên ta hãy qui nạp theo m, và áp dụng bài 1.23.

3.10. Tổng phải tính là hữu hạn số hạng vì bao giờ cũng có $k \in \mathbb{N}$ để $2^k > n$, khi ấy $n + 2^k < 2^{k+1}$ nên các số hạng từ thứ $k+1$ trở đi đều bằng 0.

Cách thứ nhất. Áp dụng bài 3.4.b vào mỗi số hạng

$$\left[\frac{n+2^k}{2^{k+1}}\right] = \left[\frac{n}{2^{k+1}} + \frac{1}{2}\right] = \left[\frac{2n}{2^{k+1}}\right] - \left[\frac{n}{2^{k+1}}\right].$$

Cách thứ hai. Gọi tổng phải tính là S_n, trong công thức của S_n thay n bởi n + 1 thì mỗi số hạng hoặc bằng chính nó, hoặc tăng thêm 1 đơn vị. Số hạng thứ r tăng thêm 1 đơn vị khi và chỉ khi

$$\left[\frac{n+1+2^r}{2^{r+1}}\right] = \left[\frac{n+2^r}{2^{r+1}}\right] + 1 = m.$$

Suy ra rằng $n < 2^r(2m-1) \leqslant n+1$ tức là $n+1 = 2^r \times \times(2m-1)$. Với mỗi số n chỉ có một số hạng thứ r như thế do đó: $S_{n+1} = S_n + 1$. Vì $S_1 = 1$ nên $S_n = n$.

3.11. a) $\alpha = 1$, $\beta = 2$, $q = 2$, $p = 3$, do đó $n = 12$. b) $n = 144$. c) $n = 75$. d) $n = 7875$. e) $\varphi(2^\alpha 3^\beta p) = 2^{\alpha-1}3^{\beta-1} \times \times 2(p-1) = 180 = 2^2 . 3^2 . 5$, tức là $2^\alpha 3^{\beta-1}(p-1) = 2^2 . 3^2 . 5$. Vì p là số nguyên tố lẻ nên $p - 1 \vdots 2$ và $p - 1 \vdots 5$. Từ đó $p - 1 = 2 . 5$ ta có $p = 11$; $p - 1 = 2.5.3$ ta có $p = 31$; $p - 1 = 2.5.3^2$ ta có $p = 91$ nhưng trường hợp này không thể được vì 91 không phải là số nguyên tố.
Với $p = 11$ có $2^\alpha 3^{\beta-1} . 10 = 2^2 3^2 . 5$ nên $\alpha = 1$, $\beta = 3$ $n = 594$;
với $p = 31$ có $\alpha = 1$, $\beta = 2$, $n = 558$.

3.12. a) Xét các cặp ước d, d' mà dd' = n. Nếu n có bao nhiêu ước $d < \sqrt{n}$ thì có ngần ấy ước $d' > \sqrt{n}$. Vậy nếu $\sqrt{n}$ không nguyên thì n có một số chẵn các ước, còn nếu $\sqrt{n} = a = a^2$ nguyên thì n có một số lẻ các ước.

Cách thứ hai. $\tau(n) = (\alpha_1 + 1)(\alpha_2 + 1)\ldots(\alpha_k + 1)$ là số chỉ khi và chỉ khi mọi α_i đều chẵn.

b) Giả sử $\sigma(n)$ là số lẻ và $n = 2^r k$ với k là số lẻ và $r \geqslant 0$. $\sigma(n) = (2^{r+1} - 1)\sigma(k)$ nên $\sigma(k)$ là lẻ. Thêm vào đó, mỗi ước của k phải là số lẻ nên $\tau(k)$ phải lẻ, theo

câu a) thì k phải là chính phương, tức là $n=2^r k$, $k=a^2$, $r \geqslant 0$. Rõ ràng hoặc $r = 0$ hoặc $r = 1$, vì nếu $r > 1$ thì $\sigma(n)$ là chẵn.

Đảo lại nếu $n = a^2$ hoặc $n = 2b^2$ thì $n = 2^{\alpha} p_1^{2\alpha_1} \ldots p_k^{2\alpha_k}$ trong đó p_i là nguyên tố lẻ. Khi ấy $\sigma(n) = (2^{\alpha+1} - 1) \times$ $\times \sigma(p_1^{2\alpha_1}) \ldots \sigma(p_k^{2\alpha_k})$ là lẻ vì $\sigma(p_i^{2\alpha_i})$ là lẻ (tổng một số lẻ các số hạng lẻ).

c) Nếu n có ít nhất một ước nguyên tố lẻ là p thì $\varphi(n)$ chia hết cho số chẵn $p - 1$. Nếu $n = 2^r$ thì $\varphi(n) = 2^{r-1}$ chia hết cho 2 vì $r > 1$.

Bây giờ giả sử m có hai hay nhiều hơn hai thừa số nguyên tố khác nhau p, q thì ta có $\varphi(n) \vdots (p-1)(q-1)$ (p, q là những số nguyên tố lẻ vì $\varphi(n)$ không là bội của 4). Chỉ cần xét với $n = 1, 2^r, p^s$. Trả lời $n = 1, 2, 4, p^s, 2p^s$ với p là số nguyên tố lẻ dạng $4k + 3$.

3.13. Với $n = p_1^{\alpha 1} p_2^{\alpha 2} \ldots p_r^{\alpha r}$ ta có

$$\sigma_k(n) = \frac{p_1^{k(\alpha_1+1)} - 1}{p_1^k - 1} \cdot \frac{p_2^{k(\alpha_2+1)} - 1}{p_2^k - 1} \ldots \frac{p_r^{k(\alpha_r+1)} - 1}{p_r^k - 1}.$$

Chú ý. Ta có $\sigma_0(n) = \sum_{d/n} 1 = \tau(n)$; $\sigma_1(n) = \sum_{d/n} d = \sigma(n)$.

3.14. a) $\prod_{d/n} d = \prod_{d/n} \left(\frac{n}{d}\right) = \frac{n^{\tau(n)}}{\prod_{d/n} d}$ $\left(\prod_{d/n} d\right)^2 = n^{\tau(n)}$.

b) $\sum_{d/n} d = \sum_{d/n} \left(\frac{n}{d}\right) = n \sum_{d/n} \frac{1}{d}$.

3.15. a) *Cách thứ nhất.* Qui nạp theo n với chú ý rằng

$$\left[\frac{n+1}{d}\right] = \begin{cases} \left[\frac{n}{d}\right] & \text{nếu d không chia hết } n+1, \\ \left[\frac{n}{d}\right] + 1 & \text{nếu d chia hết } n+1. \end{cases}$$

Cách thứ hai. $\tau(1) + \tau(2) + ... + \tau(n)$ bằng số tất cả các số d là ước của 1, hoặc 2, hoặc 3,..., hoặc n. Mặt khác số các ước $d = 1$ của dãy 1, 2,..., n bằng $\left[\frac{n}{1}\right]$, số các ước $d = 2$ của dãy 1, 2,..., n bằng $\left[\frac{n}{2}\right]$,.... Từ đó suy ra điều cần phải chứng minh.

Cách thứ ba. $\tau(1) + \tau(2) + ... + \tau(n)$ bằng số các điểm nguyên (x, y) mà $xy = 1$, $xy = 2$,..., $xy = n$ bằng số các điểm nguyên nằm giữa đường hypebôn $xy = n$ và hai bán trục ox, oy, mà số các điểm nguyên có hoành độ $x = k$ là $\left[\frac{n}{k}\right]$.

b) Có thể giải như cách thứ nhất hoặc cách thứ hai ở câu a.

3.16. a) – *Với* $n = pq$ ta có $\sigma(n) = (p+1)(q+1) = 2pq$ nên suy ra $(p - 1)(q - 1) = 2$, từ đó $n = 6$.

– *Với* $n = p^2q$ ta có $\sigma(n) = (p^2 + p + 1)(q + 1) = 2p^2q$ nên suy ra $(q - 1)(p^2 - p - 1) = 2(p + 1)$. Nhưng ta thấy $(p + 1,\ p^2 - p - 1) = 1$ cho nên $p^2 - p - 1 = 1$ hoặc $p^2 - p - 1 = 2$. Nếu $p^2 - p - 1 = 1$ thì $p = 2$, khi ấy $q = 7$, nghĩa là $n = 2^2 . 7 = 28$. Rõ ràng $n = 28$ là một số hoàn chỉnh. Nếu $p^2 - p - 1 = 2$ thì p là ước của 3, song 3 không nghiệm phương trình $p^2 - p - 3 = 0$. Vậy ta có đáp số $n = 28$.

b) Chứng minh bằng phản chứng.

— *Với* $n = p^\alpha$. Giả sử $n = p^\alpha$ là một số hoàn chỉnh thì $\sigma(n) = 2n$ thế thì $\frac{p^{\alpha+1} - 1}{p - 1} = 2 \cdot p^\alpha$

suy ra $p^{\alpha+1} - p^\alpha = p^\alpha - 1$. Đẳng thức này không thể xảy ra với p là số nguyên tố, bởi vì $p \geqslant 2$ ta có $p - 1 \geqslant 1$ cho nên $p^{\alpha+1} - p^\alpha = p^\alpha . (p - 1) \geqslant p^\alpha > p^\alpha - 1$.

— *Với* $n = p^3q$. Giả sử $n = p^3q$ là một số hoàn chỉnh thì
$$(p^3 + p^2 + p + 1)(q + 1) = 2p^3q$$
suy ra
$$(p^3 - p^2 - p - 1)(q - 1) = 2(p^2 + p + 1).$$
Nhưng $(p^3 - p^2 - p - 1, \; p^2 + p + 1) = 1$ nên hoặc $p^3 - p^2 - p - 1 = 1$ hoặc $p^3 - p^2 - p - 1 = 2$, tức là $p^3 - p^2 - p - 2 = 0$ hoặc $p^3 - p^2 - p - 3 = 0$. $p^3 - p^2 - p - 2 = 0$ có nghiệm nguyên p thì $p \mid 2$, do p là số nguyên tố ta có $p = 2$, nhưng $p = 2$ không nghiệm đúng phương trình $p^3 - p^2 - p - 2 = 0$, nói khác đi phương trình $p^3 - p^2 - p - 2 = 0$ không có nghiệm nguyên tố. Bằng lý luận tương tự phương trình $p^3 - p^2 - p - 3 = 0$ cũng không có nghiệm nguyên tố. Do đó không thể có các số hoàn chỉnh dạng $n = p^3q$.

3.17. a) $\sigma(p^\alpha) = p^\alpha + \frac{p^\alpha - 1}{p - 1} < 2p^\alpha - 1 < 2p^\alpha$.

b) Hãy lấy $n = 2^\alpha$.

c) Giả sử $n = p^\alpha q^\beta$ với p, q là những số nguyên tố lẻ phân biệt thế thì ta có
$$\sigma(p^\alpha q^\beta) = \frac{p^{\alpha+1} - 1}{p - 1} \cdot \frac{q^{\beta+1} - 1}{q - 1} < \frac{npq}{(p-1)(q-1)} < 2n.$$

Nhận xét. Từ kết quả câu a, ta có kết luận: *có vô số số thiếu.*

3.18. a) Hãy dựa vào công thức tính $\varphi(n)$

b) Giả sử $m = p_1^{\alpha 1} p_2^{\alpha 2} \dots p_k^{\alpha k}$ Khi đó ta có

$$\varphi(m^{\alpha}) = m^{\alpha} \prod_{i=1}^{k} \left(1 - \frac{1}{p_i}\right) = m^{\alpha-1}\left[m \prod_{i=1}^{k} \left(1 - \frac{1}{p_i}\right)\right] =$$

$$= m^{\alpha-1} \varphi(m).$$

3.19. a) $\sum_{i=0}^{\alpha} \varphi(p^i) = \varphi(1) + \varphi(p) + \ldots + \varphi(p^{\alpha}) =$

$$= 1 + (p - 1) + (p^2 - p) + \ldots + (p^{\alpha} - p^{\alpha-1}) = p^{\alpha}.$$

b) Giả sử $n = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_k^{\alpha_k}$, ta có $d \mid n$ khi và chỉ khi $d = p_1^{\beta_1} p_2^{\beta_2} \ldots p_k^{\beta_k}$, $0 \leqslant \beta_i \leqslant \alpha_i$, $i = 1, 2, \ldots, k$ (xem 1.IV. §2. Bài thứ hai). Bởi vậy

$$\sum_{d/n} \varphi(d) = \sum_{\substack{\beta_i = 0,1,\ldots,\alpha_i \\ i = 1, 2,\ldots, k}} \varphi(p_1^{\beta_1} p_2^{\beta_2} \ldots p_k^{\beta_k}) =$$

$$= \sum_{\substack{\beta_i = 0,1,\ldots,\alpha_i \\ i = 1, 2,\ldots, k}} \varphi(p_1^{\beta_1}) \varphi(p_2^{\beta_2}) \ldots \varphi(p_k^{\beta_k})$$

$$= \prod_{i=1}^{k} (\varphi(p_i^0) + \varphi(p_i^1) + \ldots + \varphi(p_i^{\alpha_i})) = \prod_{i=1}^{k} p_i^{\alpha_i} = n.$$

3.20. Giả sử $m > 2$ thế thì $m - 1 > 1$ và $(m - 1, m) = (1, m) = 1$ cho nên suy ra $\varphi(m) > 1$.

Bây giờ giả sử chỉ có k số nguyên tố là $p_1, p_2, \ldots, p_k$. Khi ấy mỗi số tự nhiên $x < m = p_1 p_2 \ldots p_k$ ta có x đều có ước nguyên tố p_i nào đó (giả sử $x > 1$) với $i = 1, 2, \ldots, k$, bởi vậy $\varphi(m) = 1$. Song rõ ràng $m > 2$ nên $\varphi(m) > 1$. Điều mâu thuẫn đó chứng tỏ rằng có vô số số nguyên tố.

3.21. a) Giả sử $p_1, p_2, \ldots, p_r$ là các số nguyên tố chỉ có mặt trong sự phân tích tiêu chuẩn của a ; $q_1, q_2, \ldots, q_s$

là các số nguyên tố chỉ có mặt trong sự phân tích tiêu chuẩn của b; $l_1, l_2, \ldots, l_k$ là các số nguyên tố có mặt cả trong sự phân tích tiêu chuẩn của a và b. Ta có

$$\varphi(a, b) = ab \prod_{i=1}^{r}\left(1 - \frac{1}{p_i}\right)\prod_{j=1}^{s}\left(1 - \frac{1}{q_j}\right)\prod_{t=1}^{k}\left(1 - \frac{1}{l_t}\right) =$$

$$= md \prod_{i=1}^{r}\left(1 - \frac{1}{p_i}\right)\prod_{j=i}^{s}\left(1 - \frac{1}{q_j}\right)\prod_{t=1}^{k}\left(1 - \frac{1}{l_t}\right) = d\varphi(m)$$

c) $$\varphi(ab) = ab \prod_{i=1}^{r}\left(1 - \frac{1}{p_i}\right)\prod_{j=1}^{s}\left(1 - \frac{1}{q_j}\right)\prod_{t=1}^{k}\left(1 - \frac{1}{l_t}\right) =$$

$$= \left[a \prod_{i=1}^{r}\left(1 - \frac{1}{p_i}\right)\prod_{t=1}^{k}\left(1 - \frac{1}{l_t}\right)\right] \times$$

$$\times \left[b \prod_{j=1}^{s}\left(1 - \frac{1}{q_j}\right)\prod_{t=1}^{k}\left(1 - \frac{1}{l_t}\right)\right] \cdot \frac{d}{d\prod_{t=1}^{k}\left(1 - \frac{1}{l_t}\right)} =$$

$= \varphi(a)\,\varphi(b)\,\dfrac{d}{\varphi(d)}$ từ đó $\varphi(d)\,\varphi(ab) = d\varphi(a)\varphi(b)$.

3.23. a) $\varphi(x) = 2^7$, ta có $x = 2^8$; $2^7.3$; $2^6.5$; $2^4.17$; $2^5.3.5$; $2^3.3.17$; $2^2.5.17$; $2.3.5.17$.

b) $\varphi(x) = 12$. Có ít nhất hai giá trị $x = 13$ và $x = 26$ nghiệm đúng $\varphi(x) = 12$. Bây giờ giả sử p là ước nguyên tố của x thế thì $\varphi(p) \mid \varphi(x)$ (bài tập 3.18a). Vì $\varphi(x) = 12 = 2^2.3$, nên hoặc $p = 2$, $p = 3$ hoặc $p - 1 \vdots 2$, $p - 1 \vdots 3$. Từ đó các khả năng có thể của p là $p = 2, 3, 5, 7, 11, 13$ (vì $p \leqslant 13$).

Với $p = 13$ ta có $x_1 = 13$. Hơn nữa $12 = 1.12$ mà với $q = 2$ có $\varphi(q) = 1$ nên còn có $x_2 = 26$.

Với $p = 11$ ta có $\varphi(p) = 10$ không chia hết 12.
Với $p = 7$ ta có $\varphi(p) = 6$, $\varphi(x) = 12 = 2.6$. Ta hãy xem có những ước q nào mà $\varphi(q) = 2$? $q = 5$ không được vì $\varphi(5) = 4 > 2$; $q = 3$ ta có $\varphi(3) = 2$ nên được $x_3 = p.q = 21$, $\varphi(3^2) = 6 > 2$; $q = 2$ ta có $\varphi(2) = 1$, $\varphi(2^2) = 2$ nên được $x_4 = p.q^2 = 28$, $\varphi(2^3) = 4 > 2$; $q = 2.3$ ta có $\varphi(6) = 2$ nên được $x_5 = p.q = 42$.

Với $p = 5$ ta có $\varphi(p) = 4$, $\varphi(p^2) = 20 > 12$. Với $\varphi(p) = 4$ ta hãy xét có những ước q nào mà $\varphi(q) \mid 3$, $q = 2$ có $\varphi(2) = 1$, $\varphi(2^2) = 2 < 3$, $\varphi(2^3) = 4 > 3$.

Với $p = 3$ bằng lý luận như các trường hợp ở trên ta được $x_6 = 36$.

$p = 2$ không thể xảy ra.

Trả lời: $x = 13, 21, 26, 28, 36, 42$.

∴

4.1. *Trả lời*: $\frac{127}{52} = [2; 2, 3, 1, 5]$;

$$-\frac{83}{217} = [-1; 1, 1, 1, 1, 5, 1, 2, 2];$$

$$1{,}23 = [1; 4, 2, 1, 7];$$

$$0{,}00012 = [0; 8333, 3]$$

4.2. *Trả lời*: $[0; 1, 2, 3, 4, 5] = \frac{157}{225}$;

$$[1; 10, 100, 1000, 1000] = \frac{11\,010\,111\,101}{10\,010\,101\,001};$$

$$[a; a, a, a, a] = \frac{a^5 + 4a^3 + 3a}{a^4 + 3a^2 + 1};$$

$$[a; b, a, b, a] = \frac{a^3b^2 + 4a^2b + 3a}{a^2b^2 + 3ab + 1}.$$

4.3. a) $P_s = q_sP_{s-1} + P_{s-2}$, $P_s - P_{s-2} = q_sP_{s-1}$,

$$Q_s = q_sQ_{s-1} + Q_{s-2},\ Q_s - Q_{s-2} = q_sQ_{s-1}.$$

Từ đó ta có:

$$\left(\frac{P_{s+2}}{P_s}-1\right)\left(1-\frac{P_{s-1}}{P_{s+1}}\right)=q_{s+2}\,\frac{P_{s+1}}{P_s}\cdot q_{s+1}\,\frac{P_s}{P_{s+1}}=q_{s+2}q_{s+1}\,.$$

$$\left(\frac{Q_{s+2}}{Q_s}-1\right)\left(1-\frac{Q_{s-1}}{Q_{s+1}}\right)=q_{s+2}\,\frac{Q_{s+1}}{Q_s}\cdot q_{s+1}\,\frac{Q_s}{Q_{s+1}}=q_{s+2}q_{s+1}.$$

So sánh các kết quả ở trên suy ra điều cần chứng minh.

b) Biến đổi vế trái: $P_{s+2}\,Q_{s-2}-P_{s-2}\,Q_{s+2}=$

$$\begin{aligned}
&=(q_{s+2}\,P_{s+1}+P_s)\,Q_{s-2}-P_{s-2}\,(q_{s+2}\,Q_{s+1}+Q_s)=\\
&=q_{s+2}\,(P_{s+1}\,Q_{s-2}-P_{s-2}\,Q_{s+1})+P_s\,Q_{s-2}-P_{s-2}\,Q_s=\\
&=q_{s+2}((q_{s+1}\,P_s+P_{s-1})\,Q_{s-2}-P_{s-2}\,(q_{s+1}\,Q_s+Q_{s-1}))+\\
&+(q_s\,P_{s-1}+P_{s-2})\,Q_{s-2}\;P_{s-2}\,(q_s\,Q_{s-1}+Q_{s-2})=\\
&=q_{s+2}\,q_{s+1}\,(P_s\,Q_{s-2}-P_{s-2}\,Q_s)+q_{s+2}\,(P_{s-1}\,Q_{s-2}-\\
&-P_{s-2}\,Q_{s-1})+q_s\,(P_{s-1}\,Q_{s-2}-P_{s-2}\,Q_{s-1})=\\
&=q_{s+2}\,q_{s+1}((q_s\,P_{s-1}+P_{s-2})\,Q_{s-2}-P_{s-2}(q_s\,Q_{s-1}+\\
&+Q_{s-2}))+q_{s+2}\,(-1)^s+q_s(-1)^s=\\
&=q_{s+2}\,q_{s+1}\,q_s\,(P_{s-1}\,Q_{s-2}-Q_{s-1}\,P_{s-2})+q_{s+2}(-1)^s+\\
&+q_s\,(-1)^s=(-1)^s\,(q_{s+2}\,q_{s+1}\,q_s+q_{s+2}+q_s).
\end{aligned}$$

c) Bởi vì $\dfrac{P_k}{Q_k}-\dfrac{P_{k-1}}{Q_{k-1}}=(-1)^{k-1}\dfrac{1}{Q_k\,Q_{k-1}}$ nên ta có

$$\frac{P_s}{Q_s}-\frac{P_0}{Q_0}=\frac{P_s}{Q_s}-\frac{P_{s-1}}{Q_{s-1}}+\frac{P_{s-1}}{Q_{s-1}}-\frac{P_{s-2}}{Q_{s-2}}+\dots+$$

$$+\frac{P_1}{Q_1}-\frac{P_0}{Q_0}=\frac{(-1)^{s-1}}{Q_{s-1}\,Q_s}+\frac{(-1)^{s-2}}{Q_{s-2}\,Q_{s-1}}+\dots+\frac{1}{Q_0Q_1}\,.$$

4.4. a) $\dfrac{P_n}{P_{n-1}}=\dfrac{q_nP_{n-1}+P_{n-2}}{P_{n-1}}=q_n+\dfrac{1}{\dfrac{P_{n-1}}{P_{n-2}}}$

$$\frac{P_{n-1}}{P_{n-2}}=q_{n-1}+\frac{1}{\dfrac{P_{n-2}}{P_{n-3}}}\,,\dots,\;\frac{P_1}{P_0}=\frac{q_1q_0+1}{q_0}=q_1+\frac{1}{q_0}\,.$$

Từ đó ta có:

$$\frac{P_n}{P_{n-1}} = [q_n;\ q_{n-1}, \dots, q_o].$$

b) Tương tự vì $\dfrac{Q_n}{Q_{n-1}} = q_n + \dfrac{1}{\dfrac{Q_{n-1}}{Q_{n-2}}}, \dots, \dfrac{Q_1}{Q_o} = q_1$

nên ta có

$$\frac{Q_n}{Q_{n-1}} = [q_n;\ q_{n-1}, \dots, q_1].$$

Chú ý. Có thể chứng minh bằng phép qui nạp theo n.

4.5. a) Gọi $(P_s, P_{s-1}) = d$. Từ $P_s = q_s P_{s-1} + P_{s-2}$ ta suy ra rằng $(P_{s-1}, P_{s-2}) = (P_s, P_{s-1}) = d$ và cứ tiếp tục lập luận ấy ta sẽ có $(P_1, P_o) = d$. Như vậy $d = (P_1, P_o) = (q_1q_o + 1, q_o) = (1, q_o) = 1$, và do đó $(P_s, P_{s-1}) = 1$.

b) *Chỉ dẫn*. Chứng minh tương tự câu a).

4.6. *Chỉ dẫn*. Hãy qui nạp theo n.

4.7. Áp dụng bài tập 4.4 ta có

$$\frac{P_n}{P_{n-1}} = [q_n;\ q_{n-1}, \dots, q_1]$$

và theo giả thiết ta được $\dfrac{P_n}{P_{n-1}} = \dfrac{P_n}{Q_n}$. Từ đó do $P_n \neq 0$ ta được $P_{n-1} = Q_n$.

4.8. a) Ta có $\sqrt{3} = [1;\ (1, 2)]$ và bảng các giản phân đầu tiên của nó là:

q_s	1	1	2	1	2	1	2	...
$\frac{P_s}{Q_s}$	$\frac{1}{1}$	$\frac{2}{7}$	$\frac{5}{3}$	$\frac{7}{4}$	$\frac{19}{11}$	$\frac{26}{15}$	$\frac{71}{41}$	...

Từ $\left|\alpha - \frac{P_s}{Q_s}\right| < \frac{1}{Q_s Q_{s+1}} < \frac{1}{Q_s^2} < 0{,}001$ suy ra rằng

$Q_s^2 > 1000$ tức là $Q_s > 33$. Vậy có thể lấy số hữu tỷ xấp xỉ tốt nhất của $\sqrt{3}$ với sai số tuyệt đối nhỏ hơn 0,001 là $\frac{71}{41}$.

b) Ta có $\sqrt{11} = [3; (3, 6)]$, bảng các giản phân đầu tiên của nó là

q_s	3	3	6	3	6	...
$\frac{P_s}{Q_s}$	$\frac{3}{1}$	$\frac{10}{3}$	$\frac{63}{19}$	$\frac{199}{60}$	$\frac{1257}{379}$	...

Trả lời : Số hữu tỷ cần tìm có thể là $\frac{199}{60}$.

4.9. *Cách thứ nhất :* Dựa vào hằng đẳng thức

$$(\sqrt{a^2+1} - a)(\sqrt{a^2+1} + a) = 1$$

ta có

$$\sqrt{a^2+1} - a = \frac{1}{\sqrt{a^2+1} + a}$$

hay là :

$$\sqrt{a^2+1} - a = \frac{1}{2a + \sqrt{a^2+1} - a}.$$

Thay biểu thức của $\sqrt{a^2+1} - a$ liên tiếp ta được

$$\sqrt{a^2+1} - a = \cfrac{1}{2a + \cfrac{1}{2a + \cfrac{1}{2a + .}}}$$

cuối cùng ta được

$$\sqrt{a^2+1} = a + \cfrac{1}{2a + \cfrac{1}{2a + \cfrac{1}{2a + \dots}}}$$

Cách thứ hai. Gọi $\alpha = [a; (2a)]$ ta có $\alpha = [a; \alpha_1] = a + \dfrac{1}{\alpha_1}$, trong đó $\alpha_1 = [2a; 2a, 2a, \dots] = 2a + \dfrac{1}{\alpha_1}$.

Từ đó ta có $\alpha = \dfrac{a\alpha_1 + 1}{\alpha_1}$ và $\alpha_1 = \dfrac{2a\alpha_1 + 1}{\alpha_1}$, tức là $\alpha_1 = \dfrac{1}{\alpha - a}$ và $\alpha_1^2 - 2a\alpha_1 - 1 = 0$. Thay α_1 theo α ta có $\alpha^2 - a^2 - 1 = 0$. Vì $0 < a < \alpha$ ta được $\alpha = \sqrt{a^2+1}$.

4.10. a) Đặt $\alpha = [2; 3, (2,1)]$ và $x = [2; (1, 2)]$ ta có : $\alpha = 2 + \cfrac{1}{3 + \cfrac{1}{x}}$; $x = 2 + \cfrac{1}{1 + \cfrac{1}{x}}$ và $2 < x < 3$.

Ta có phương trình theo x là $x^2 - 2x - 2 = 0$, với điều kiện $2 < x < 3$ ta được $x = 1 + \sqrt{3}$. Từ đó $\alpha = 2 + \cfrac{1}{3 + \cfrac{1}{1+\sqrt{3}}} = \dfrac{27 - \sqrt{3}}{11}$.

b) $\dfrac{10 - \sqrt{2}}{14}$.

c) Đặt $\alpha = [a; (b, a)] = a + \cfrac{1}{b + \cfrac{1}{\alpha}}$, $\alpha > a$, ta có $b\alpha^2 - ab\alpha - a = 0$. Từ đó vì $a > 0$, $\alpha > a > 0$ ta được

$$\alpha = \frac{ab + \sqrt{a^2b^2 + 4ab}}{2b}.$$

4.11. Đặt $\alpha = [a ; b, a, b, \ldots]$ ta có $[0 ; b, a, \ldots] = \alpha - a$. Theo như lý luận ở bài tập 4.10.c, ta được

$$b\alpha^2 - ab\alpha - a = 0$$

hay

$$\alpha(\alpha - a) = \frac{a}{b}.$$

4.12. Với $s \geqslant 2$ ta có

$$Q_s = q_s Q_{s-1} + Q_{s-2} \geqslant Q_{s-1} + Q_{s-2} \geqslant 2Q_{s-2}.$$

Áp dụng hệ thức này với $s = 2k$ và $s = 2k + 1$ ta được

$$Q_{2k} \geqslant 2^k Q_o = 2^k \geqslant 2^{k - \frac{1}{2}} = 2^{\frac{2k-1}{2}}$$

$$Q_{2k+1} \geqslant 2^k Q_1 \geqslant 2^k = 2^{\frac{(2k+1)-1}{2}}.$$

Như vậy với $s \geqslant 2$ ta có $Q_s \geqslant 2^{\frac{s-1}{2}}$.

Cách thứ hai : qui nạp theo s.

Với $s = 2$ ta có $Q_2 \geqslant 2Q_o = 2 > \sqrt{2} = 2^{\frac{2-1}{2}}$.

Giả sử $Q_k \geqslant 2^{\frac{k-1}{2}}$, $2 \leqslant k < s$. Khi ấy

$$Q_s \geqslant 2Q_{s-2} \geqslant 2 \cdot 2^{\frac{(s-2)-1}{2}} = 2^{\frac{s-1}{2}}.$$

4.13. Giả sử $\alpha = [q_o ; q_1, q_2, \ldots]$ và ta có dãy

$$1 = Q_o < Q_1 < Q_2 < \ldots$$

Ta nhận thấy có thể xảy ra :

Có chỉ số i nào đó sao cho $Q_i \leqslant \tau < Q_{i+1}$. Khi ấy

$|\alpha - \delta_i| < \dfrac{1}{Q_i Q_{i+1}} < \dfrac{1}{Q_i \tau}$, nên ta có thể lấy

$\frac{a}{b} = \delta_i = \frac{P_i}{Q_i}$, rõ ràng $\left|\alpha - \frac{a}{b}\right| < \frac{1}{b\tau}$, $0 < b < \tau$.

Nếu không có chỉ số i nào để $Q_i \leqslant \tau < Q_{i+1}$ thì có nghĩa là dãy $1 = Q_0 < Q_1 < Q_2 < \dots$ dừng, ta được điều tương đương là $\alpha = [q_0; q_1, q_2, \dots, q_n]$. Khi ấy rõ ràng $Q_n < \tau (\tau > 1)$ nên $|\alpha - \delta_n| = 0 \leqslant \frac{1}{Q_n \tau}$, do đó với $\frac{a}{b} = \delta_n$ ta có

$$\left|\alpha - \frac{a}{b}\right| < \frac{1}{b\tau},\ 0 \leqslant b = Q_n < \tau.$$

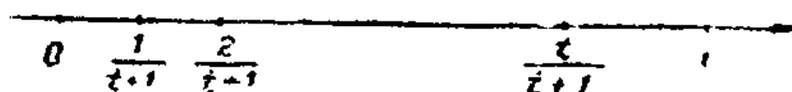
Cách thứ hai (Điriclê). Giả sử $t = [\tau]$. Chúng ta xét tập hợp $t + 2$ số gồm các giá trị phần phân $\{x\alpha\}$, $x = 0, 1, \dots, t$, và số 1 (trong đó như ta đã biết

$$\{x\alpha\} = x\alpha - [x\alpha],\ 0 \leqslant \{x\alpha\} < 1).$$

Hiển nhiên mỗi một trong các số của tập hợp này phải thuộc một và chỉ một trong $t + 1$ khoảng

$$\left[0, \frac{1}{t+1}\right), \left[\frac{1}{t+1}, \frac{2}{t+1}\right), \left[\frac{2}{t+1}, \frac{3}{t+1}\right), \dots, \left[\frac{t}{t+1}, 1\right]$$

(các khoảng đầu là nửa đoạn, khoảng cuối là đoạn).



Bởi vì có $t + 2$ số nên nhất thiết ắt có một khoảng chứa hai số trong tập hợp $\{\{x\alpha\}, 1\}$ $(x = 0, 2, \dots, t)$. Hiệu của hai số này không vượt quá độ dài của khoảng chứa chúng, nghĩa là $\leqslant \frac{1}{t+1} < \frac{1}{\tau}$.

Nếu $\{x_1\alpha\}$ và $\{x_2\alpha\}$ là các số như vậy thì

$$|\{x_2\alpha\} - \{x_1\alpha\}| = |(x_2 - x_1)\alpha - ([x_2\alpha] - [x_1\alpha])| < \frac{1}{\tau}.$$

Giả sử $x_2 > x_1$, ta đặt $b = x_2 - x_1$ và $[x_2\alpha] - [x_1\alpha] = a$ thì rõ ràng $0 < b \leqslant t \leqslant \tau$ và $|b\alpha - a| < \frac{1}{\tau}$, tức là

$$\left|\alpha - \frac{a}{b}\right| < \frac{1}{b\tau}$$

Nếu $\{x_3\alpha\}$ và 1 cùng thuộc một khoảng thì $|1 - \{x_3\alpha\}| = |1 - x_3\alpha + [x_3\alpha]| = |x_3\alpha - (1 + [x_3\alpha])| < \frac{1}{\tau}$. Bằng cách đặt $x_3 = b$, $1 + [x_3\alpha] = a$ thì rõ ràng $0 < b \leqslant t \leqslant \tau$ và $|b\alpha - a| < \frac{1}{\tau}$, tức là

$$\left|\alpha - \frac{a}{b}\right| < \frac{1}{b\tau}.$$

Chú ý. Nội dung của định lý này: với số thực α tùy ý và $\tau \geqslant 1$ tùy ý, ắt có số hữu tỉ $\frac{a}{b}$ gần đúng α sai số tuyệt đối nhỏ hơn $\frac{1}{b\tau}$, trong đó $0 < b \leqslant \tau$.

Chẳng hạn đối với $\sqrt{19}$ có $\frac{a}{b}$ gần đúng nó với sai số $\frac{1}{1000b}$, trong đó b không vượt quá 1000.

– Áp dụng: Hãy xấp xỉ $\sqrt{19}$ bởi phân số $\frac{a}{b}$ sao cho sai số tuyệt đối nhỏ hơn $\frac{1}{100b}$. Ta có

$$\sqrt{19} = [4; (2, 1, 3, 1, 2, 8)]$$

q_s	4	2	1	3	1	2	8	...
$\frac{P_s}{Q_s}$	$\frac{4}{1}$	$\frac{9}{2}$	$\frac{13}{3}$	$\frac{48}{11}$	$\frac{61}{14}$	$\frac{170}{39}$	$\frac{1421}{326}$	...

Ta nhận thấy mẫu số Q_s lớn nhất $\leqslant 100$ là 39, bởi vậy có thể lấy $\frac{a}{b} = \frac{170}{39}$ ta có $\left|\sqrt{19} - \frac{170}{39}\right| < \frac{1}{100.39}$.

4.14. a) Hai nghiệm của $2x^2 - 10x + 7 = 0$ là

$$x_1 = \frac{5 + \sqrt{11}}{2}, \quad x_2 = \frac{5 - \sqrt{11}}{2}.$$

$$x_1 = [4; (6, 3)], \quad x_2 = [0; 1, 5, (3, 6)].$$

Từ $\left|\alpha - \frac{P_s}{Q_s}\right| < \frac{1}{Q_sQ_{s+1}} < \frac{1}{Q_s^2} < (0,1)^4$

suy ra $Q_s > 100$.

x_1	q_s	4	6	3	6	3
	$\frac{P_s}{Q_s}$	$\frac{4}{1}$	$\frac{25}{6}$	$\frac{79}{19}$	$\frac{499}{120}$	...

x_2	q_s	0	1	5	3	6
	$\frac{P_s}{Q_s}$	$\frac{0}{1}$	$\frac{1}{1}$	$\frac{5}{6}$	$\frac{16}{19}$	$\frac{101}{120}$

Vậy có thể lấy $x_1 \approx \frac{499}{120}$ $(+ 0,0001)$.

$$x_2 \approx \frac{101}{120} \ (- 0,0001).$$

b) $|x_1| = \frac{5 - \sqrt{2}}{2} = [1; 1, 3, (1, 4)] \approx \frac{251}{125}$ $(-0,0001)$

$$|x_2| = \frac{5 + \sqrt{2}}{2} = [3; (4, 1)] \approx \frac{449}{140} \ (+ 0,0001)$$

từ đó ta có

$$x_1 \approx -\frac{251}{125}\ (+\ 0{,}0001)\ \text{và}\ x_2 \approx -\frac{449}{140}\ (-\ 0{,}0001).$$

4.15. a) $\alpha = [1; (1)] = [1 : \alpha]$, $\alpha = 1 + \dfrac{1}{\alpha}$, $\alpha > 1$. Từ đó $\alpha^2 - \alpha - 1 = 0$, $\alpha > 1$ cho nên

$$\alpha = \frac{1 + \sqrt{5}}{2}.$$

b) Ta có $U_{n+2} = U_{n+1} + U_n$, $n = 1, 2, \ldots$; $U_1 = U_2 = 1$.

$$\frac{P_0}{Q_0} = \frac{1}{1} = \frac{U_2}{U_1};\ \frac{P_1}{Q_1} = \frac{2}{1} = \frac{U_1 + U_2}{U_2} = \frac{U_3}{U_2}.$$

Giả sử $\dfrac{P_{s-1}}{Q_{s-1}} = \dfrac{U_{s+1}}{U_s}$ xảy ra với $0 \leqslant s < n$. Khi ấy

$$\frac{P_n}{Q_n} = \frac{q_n P_{n-1} + P_{n-2}}{q_n Q_{n-1} + Q_{n-2}} = \frac{1.\ U_{n+1} + U_n}{1.\ U_n + U_{n-1}} = \frac{U_{n+2}}{U_{n+1}}.$$

c) Hãy qui nạp theo n với chú ý rằng

$$a = \frac{1 + \sqrt{5}}{2},\ b = \frac{1 - \sqrt{5}}{2}$$

và $U_n = U_{n-1} + U_{n-2} = \dfrac{1}{\sqrt{5}}((a^{n-1} - b^{n-1}) + (a^{n-2} - b^{n-2})) = \dfrac{1}{\sqrt{5}}\left(a^{n-1}\left(1 - \dfrac{1}{a}\right) - b^{n-1}\left(1 - \dfrac{1}{b}\right)\right) =$

$$= \frac{1}{\sqrt{5}}(a^n - b^n).$$

5.1. a) $x = 1 + 3t$, $y = -1 - 5t$; $t = 0, \pm 1, \ldots$

b) $x = 2 + 5t$, $y = 1 + t$, $t = 0, \pm 1, \ldots$

c) $\dfrac{38}{117} = [0; 3, 12, 1, 2]$

q_s	0	3	12	1	2
$\dfrac{P_s}{Q_s}$	$\dfrac{0}{1}$	$\dfrac{1}{3}$	$\dfrac{12}{37}$	$\dfrac{13}{40}$	$\dfrac{38}{117}$

$P_{n-1} = 13$, $Q_{n-1} = 46$, $n = 4$, bởi vậy

$$\begin{cases} x_0 = -8360, \\ y_0 = 2717. \end{cases} \qquad \begin{cases} x = -8360 - 117t, \\ y = 2717 + 38t \end{cases}$$

$$t = 0, \pm 1, \ldots$$

d) $(258, 175) = 1$. $-\dfrac{258}{175} = [-2; 1, 2, 9, 4, 2]$

$n = 5$, $P_4 = -115$, $Q_4 = 78$, $x_0 = -78.113$, $y_0 = -115.113$, từ đó ta được

$$\begin{cases} x = -78.113 + 175t, \\ y = -115.113 + 258t, \ t = 0, \pm 1, \ldots \end{cases}$$

e) $(1657, 367) = 1$, $\dfrac{1657}{367} = [4; 1, 1, 16, 5, 2]$, $n = 5$,

$P_4 = 754$, $Q_4 = 167$, $x_0 = 167.23$, $y_0 = 754.23$, từ đó ta được

$$\begin{cases} x = 167.23 + 367t, \\ y = 754.23 + 1657t, \ t = 0, \pm 1, \ldots \end{cases}$$

5.2. a) $(6, 11) = 1$; $x_0 = 2m + 4$, $y_0 = -m - 2$

$$\begin{cases} x = 2m + 4 + 11t, \\ y = -m - 2 - 6t, \ t = 0, \pm 1, \ldots \end{cases}$$

b) Phương trình có nghiệm nguyên khi và chỉ khi $m = 5k + 3$, k là nguyên. Khi ấy

$$\begin{cases} x = 4k + 2 + 5t \\ y = -2k - 1 - 3t, \ t = 0, \pm 1, \ldots \end{cases}$$

c) $$\begin{cases} x = 1 + \dfrac{m-2}{d} t, \\ y = -1 + \dfrac{3}{d} t, \ t = 0, \pm 1, \ldots \text{ và} \end{cases}$$

$$d = (3, m - 2) = 1; 3.$$

($d = 3 \Leftrightarrow m = 3q + 2$, $q \in Z$ và $d = 1 \Leftrightarrow m = 3q$ hoặc $m = 3q + 1$, $q \in Z$).

đ) $\begin{cases} x = m + \dfrac{2m-1}{d} t, \\ y = -1 - \dfrac{3}{d} t, \ t = 0, \pm 1, ... \end{cases}$ và

$d = (3, 2m - 1) = 1 : 3.$

e) Ta có $d = (5, 1 + 3m) = 1$ hoặc 5.
Nếu $m = 5k + 3$ thì $d = 5$, nhưng khi ấy $2m + 1 = 5l + 2$ không chia hết cho $d = 5$ nên phương trình vô nghiệm. Nếu $m \neq 5k + 3$ thì $d = 1$, khi ấy phương trình đã cho có nghiệm nguyên. Xét những trường hợp có thể $m = 5k + r$ $(r = 0, 1, 2, 4)$ ta sẽ được công thức nghiệm tương ứng trong các trường hợp ấy.

5.3. Từ $a^n + b^n = c$ và $(a, b, c) = 1$ ta có $(a, b) = 1$ và $a \cdot a^{n-1} + b \cdot b^{n-1} = c$, bởi vậy ta được

$$\begin{cases} x = a^{n-1} + bt, \\ y = b^{n-1} - at, \ t = 0, \pm 1, ... \end{cases}$$

5.4. Bài toán đưa về giải phương trình nguyên $17y = 5x + 2$ hay $17y - 5x = 2$. Nghiệm nguyên của phương trình này là

$$\begin{cases} x = 3 + 17t, \\ y = 1 + 5t, \ t = 0, \pm 1... \end{cases}$$

Trả lời: $x = 3 + 17t$, $t = 0, \pm 1, ...$

5.5. Giả sử m, n là hai số nguyên dương và a, b là hai số nguyên tố khác nhau lớn hơn $m + n$. Giả sử $c = am + bn$, $x = m$, $y = n$ là nghiệm nguyên dương duy nhất của phương trình $ax + by = c$. Thật vậy, giả sử x_1, y_1 là nghiệm nguyên dương khác của phương trình, tức là $ax_1 + by_1 = c$, thì không thể đồng thời $x_1 \geqslant m$, $y_1 > n$ hoặc $x_1 > m$, $y_1 \geqslant n$ vì khi ấy $ax_1 + by_1 > am + bn = c$. Do đó hoặc $0 < x_1 < m$ hoặc $0 < y_1 < n$. Nếu $x_1 < m$ thì $0 < m - x_1 < m$ và $ax_1 + by_1 = am + bn$ nên $by_1 = a(m - x_1) + bn$, nghĩa

là $b \mid a(m - x_1)$. Nhưng $(a, b) = 1$ kéo theo $b \mid m - x_1$ là điều không thể xảy ra được với $b > m$. Tương tự nếu $y_1 < n$ ta cũng đi đến mâu thuẫn.

5.6. Thật vậy, chẳng hạn phương trình $x + y = m + 1$ có đúng m nghiệm nguyên dương

$$\begin{cases} x = t, \\ y = m - t + 1, \; t = 1, 2, \ldots, m. \end{cases}$$

5.7. *Trả lời*: a) $\begin{cases} x = 6 - u - 3t, \\ y = 1 - u + 2t, \\ z = u, \; u = 0, \pm 1, \ldots, \; t = 0, \pm 1, \ldots \end{cases}$

b) $\begin{cases} x = 9 - 15u + 53t, \\ y = 2 - 5u + 23t, \\ z = u \; ; \; u, t = 0, \pm 1, \ldots \end{cases}$

5.8. a) $\begin{cases} x = 1 + 12t, \\ y = -1 - 3t, \\ z = 1 + 6t \; ; \; t = 0, \pm 1, \ldots \end{cases}$

b) $$\begin{cases} x = -1 - 9t, \\ y = -1 - 6t, \\ z = 2 + 5t \; ; \; t = 0, \pm 1, \ldots \end{cases}$$

c) $$\begin{cases} x = 1 - 2t, \\ y = 2 + 3t, \\ z = -1 - 5t \; ; \; t = 0, \pm 1, \ldots \end{cases}$$

d) $$\begin{cases} x = 6 - 24t, \\ y = 4 - 15t, \\ z = -1 + 5t \; ; \; t = 0, \pm 1 \ldots \end{cases}$$

e) $$\begin{cases} x = 1 + t \\ y = t \\ z = t \; ; \; t = 0, \pm 1 \ldots \end{cases}$$

5.9. a) Phương trình đầu cho ta $x = 1 + 2t$, $y = -1 - 3t$, t nguyên, từ đây với phương trình thứ hai ta có

$$(m + 1) z - 12t = m + 1.$$

Phương trình này cho ta

$t = \frac{m+1}{d} t_1$, $z = 1 + \frac{12}{d} t_1$ với $d = (m+1, 12)$, t_1 nguyên.

Từ đó
$$\begin{cases} x = 1 + \frac{2(m+1)}{d} t_1, \\ y = -1 - \frac{3(m+1)}{d} t_1, \\ z = 1 + \frac{12}{d} t_1 ; \end{cases}$$
$d = (m + 1, 12)$, t_1 là số nguyên tùy ý.

d) Phương trình đầu là $3x - 5y = 1 + 3z$, với z là số nguyên tùy ý. Ta có:
$$\begin{cases} x = 2 + 6z + 5t, \\ y = 1 + 3z + 3t, \ t \text{ nguyên}. \end{cases}$$
Từ đây với phương trình thứ hai ta có
$$t - (m + 1) z = m$$
và ta được
$$\begin{cases} z = -1 + u, \\ t = -1 + (m + 1) u, \ u \text{ là nguyên}. \end{cases}$$
Cuối cùng ta có
$$\begin{cases} x = 5mu + 11u - 9, \\ y = 3mu + 6u - 5, \\ z = -1 + u, \ u \text{ là nguyên}. \end{cases}$$

5.10. a) Ta phải có $u, v \in Z$ sao cho $x = 9u$, $x + 1 = 25v$, từ đó $25v - 9u = 1$, ta được $v = 4 + 9t$, $u = 11 + 25t$, với $0 \leqslant t \in Z$ (vì $x > 0$). Từ đây suy ra $x = 99 + 225t$, $t = 0, 1, \ldots$ b) Giả sử $x = 21u$, $x + 1 = 165v$, $u, v \in Z$. Khi ấy suy ra $165v - 21u = 1$. Không thể có $u, v \in Z$ thỏa mãn đẳng thức $165v - 21u = 1$ vì $(165, 21) = 3$ không chia hết 1.

c) Theo câu a) ta có $x = 99 + 225t$, $t = 0, 1, 2, \ldots$ thỏa mãn x bội của 9, $x + 1$ bội của 25. Khi ấy $x + 2 = 101 + 225t$. Ta phải có $225t + 101 = 4z$, $4z - 225t = 101$. Từ đây $t = 101 + 4k$, $k \geqslant 26$. Vậy $x = -22626 + 900k$, $k = 26, 27, \ldots$

5.11. Ta có $10^4x + 10^3x + 10^2x + 10x + x = 16(10^3y + 10^2y + 10y + y) + r$ và $10^3x + 10^2x + 10x + x = 16(10^2y + 10y + y) + r - 2000$. Suy ra từ đó rằng $5x = 8y + 1$, $1 \leqslant x, y \leqslant 9$.

Trả lời: $x = 5$; $y = 3$.

5.12. Số đó là 91.

5.13. Các số nguyên phải tìm là $x = 209t + 23$, $t = 0, 1, \ldots$

5.14. $$\begin{cases} 3x - 1 = 7u \\ 7x - 1 = 5v,\ u, v \in Z \end{cases}$$

Giải ra tìm được $x = -2 + 35t$, $t \in Z$

5.15. 112, 812, 532, 252, 952, 672, 392.

5.16. $$\begin{cases} x = 3 + 7u \\ y = 5 + 7v, \end{cases}$$ u, v là những số nguyên.

5.17. $x = -4 + 13t$, $0 \leqslant t \leqslant 4$.

Đáp số: $(-4; -2)$, $(9; 6)$, $(22; 14)$, $(35; 22)$ $(48; 30)$

5.20. Gọi số phải tìm là x, ta có

$$x = 4x_1 + 3 = 5x_2 + 4 = 7x_3 + 5,$$

với x_1, x_2, x_3 là nguyên. Từ đó $x = 19 + 140t$, t nguyên.

Đáp số: $x = 299$; 439.

5.21. Số phải tìm là $x = 262$.

5.22. Phải giải hệ

$$x = 2 + 5y_1 = 1 + 8y_2 = 3 + 11y_3.$$

Giải ra tìm được $x = 377 + 440t$, t nguyên.

5.23. $(x = 41 + 105u; y = 24 + 30v)$ với $u, v \in Z$

5.24. *Chỉ dẫn*

a) $\sqrt{3} = [1; (1, 2)]$; $x_1 = 2$, $y_1 = 1$.

b) $\sqrt{6} = [2; (2, 4)]$; $x_1 = 5$; $y_1 = 2$.

c) $\sqrt{13} = [3; (1, 1, 1, 1, 6)]$; $x_1 = 649$, $y_1 = 180$.

d) $\sqrt{31} = [5; (1, 1, 3, 5, 3, 1, 1, 10)]$; $x_1 = 1520$, $y_1 = 273$.

e) $\sqrt{41} = [6; (2, 2, 12)]$, $x_1 = 2049$, $y_1 = 320$, trong đó (x_1, y_1) là nghiệm nguyên nhỏ nhất.

5.25. Đặt $u = 3x - 2y$, $v = y - x$ ta có $x = u + 2v$, $y = u + 3v$. Khi ấy $u^2 - 6v^2 = 3x^2 - 2y^2 = 1$. Phương trình $u^2 - 6v^2 = 1$ có nghiệm nguyên là

$$\begin{cases} u_n = \pm \frac{1}{2}((5 + 2\sqrt{6})^n + (5 - 2\sqrt{6})^n), \\ v_n = \pm \frac{1}{2\sqrt{6}}((5 + 2\sqrt{6})^n - (5 - 2\sqrt{6})^n), n = 0, 1, 2, \ldots \end{cases}$$

Từ đó suy ra x, y theo $x = u + 2v$, $y = u + 3v$.

2.26. *Chỉ dẫn*. Giả sử x, y là nghiệm nguyên của phương trình đã cho thì

$$6x^2 + 3 = (2y + 1)^2,$$

từ đó suy ra $2y + 1$ chia hết cho 3 nghĩa là $2y + 1 = 3t$, $t \in \mathbf{Z}$. Khi ấy ta có $3t^2 - 2x^2 = 1$.

Mặt khác nếu t, x là những số nguyên thỏa mãn đẳng thức sau cùng ở trên thì t và cả 3 t phải là số lẻ nên có thể đặt $3t = 2y + 1$, $y \in \mathbf{Z}$. Từ đó

$$(2y + 1)^2 = 9t^2 = 3(2x^2 + 1) = 6x^2 + 3.$$

Nói khác đi x, y là nghiệm của phương trình đã cho.

Hãy tìm x, t từ phương trình $3t^2 - 2x^2 = 1$ (xem bài tập 5.25). Từ đó sẽ được x ; $y = \frac{3t - 1}{2}$ là nghiệm phải tìm. Chẳng hạn $x = 11$, $y = 13$ là nghiệm nguyên nhỏ nhất của phương trình đã cho.

5.27 *Chỉ dẫn*: Giả sử $2n + 1 = x^2$, $3n + 1 = y^2$, trong đó $x, y \in \mathbf{N}$ ta có $3x^2 - 2y^2 = 1$ và $n = y^2 - x^2$. Hãy tìm x, y từ phương trình $3x^2 - 2y^2 = 1$ (xem bài tập 5.25) và từ đó suy ra $n = y^2 - x^2$.

5.28. Hiển nhiên $x = 1$, $y = 1$ là một nghiệm của phương trình đã cho. Từ phương trình đã cho ta có

$$x = \frac{-1 \pm \sqrt{8y^2 + 1}}{2} \text{ do đó } 8y^2 + 1 = z^2,\ z^2 - 2(2y)^2 = 1.$$

Bằng cách đặt $2y = u$ ta đi đến giải phương trình Pell $z^2 - 2u^2 = 1$ (xem ví dụ §2. I.2). Từ đó suy ra nghiệm của phương trình đã cho.

5.29. Từ phương trình $\left[\frac{x(x+1)}{2}\right]^2 = \frac{y(y+1)}{2}$

ta đi đến $$y = \frac{-1 + \sqrt{2x^2(x+1)^2 + 1}}{2}.$$

Đặt $x(x + 1) = z$, ta có $2z^2 + 1 = t^2$, $t^2 - 2z^2 = 1$. Giải phương trình Pell ta được $z = 2; 12; 70; 408; \ldots$ Từ phương trình $x(x + 1) = 2$ ta có $x = 1$, *số tam giác* là số 1. Từ phương trình $x(x + 1) = 12$, ta có $x = 3$, *số tam giác* là số 6. Các giá trị $z = 70$, $z = 408$ không tìm được số tam giác.

Chứng minh được rằng ngoài số 1 và 6 không có *số tam giác* nào khác nữa thỏa mãn bài toán đặt ra.

5.30. *Chỉ dẫn.* Với m là một số nguyên dương ta có $x = 2m^2 + 1$, $y = 2m$ là một nghiệm nguyên của phương trình đã cho bởi vì
$$(2m^2 + 1)^2 - A(2m)^2 = 1,$$
trong đó $A = m^2 + 1$

Mặt khác ta có hằng đẳng thức
$$(x^2 + Ay^2)^2 - A(2xy)^2 = (x^2 - Ay^2)^2$$
cho nên nếu x_0, y_0 là một nghiệm nguyên của phương trình đã cho nghĩa là $x_0^2 - Ay_0^2 = 1$ thì $x_1 = x_0^2 - Ay_0^2$, $y_1 = 2x_0y_0$ cũng là nghiệm nguyên của phương trình đã cho.

5.31. *Chỉ dẫn* : Xem cách giải phương trình $x^2 - Ay^2 = 1$. Giả sử $\sqrt{A} = [q_0; (q_1, q_2, \ldots, q_m, 2q_0)]$ là khai triển thành liên phân số của $\sqrt{A}$ và P_n, Q_n là tử số và mẫu số của giản phân thứ n của liên phân số ấy, ta có
$$P_n^2 - AQ_n^2 = (-1)^{n-1}$$
(xem §2. I.3), từ đó ta có:

— nếu n chẵn thì P_n, Q_n là một nghiệm nguyên dương của phương trình đã cho;

— nếu n lẻ thì P_{2n+1}, Q_{2n+1} là một nghiệm nguyên dương của các phương trình đã cho.

Tập hợp nghiệm nguyên của phương trình đã cho được xác định như tập hợp nghiệm nguyên của phương trình

$$x^2 - Ay^2 = 1$$

đã nêu ở phần lý thuyết.

5.32. $x_1 = 7, \quad y_1 = 5.$

5.33. *Chỉ dẫn*: Từ phương trình đã cho ta thấy x phải là số chẵn. Đặt $x = 2x_1$, ta được $2x_1^2 - y^2 = 1$, $y^2 - 2x_1^2 = -1$ đưa phương trình đang xét về giải phương trình Pell.

5.34. Rõ ràng đường tròn và đường thẳng có một điểm chung $A(0; -1)$. Nếu cả giao điểm thứ hai $B(x, y)$ cũng là hữu tỷ thì $k = \frac{y+1}{x}$ cũng là hữu tỷ (vì $x \neq 0$). Ngược lại nếu k là số hữu tỷ thì tọa độ x, y của giao điểm B(x, y) của đường tròn và đường thẳng thỏa mãn hệ thức $x^2 + (kx - 1)^2 = 1$. Khi ấy $x = \frac{2k}{k^2+1}$ và do đó $y = \frac{k^2-1}{k^2+1}$, ta có x, y là những số hữu tỷ, nói khác đi B là điểm hữu tỷ của đường tròn $x^2 + y^2 = 1$.

b) Vấn đề tìm nghiệm nguyên của phương trình $x^2 + y^2 = z^2$ tương đương với vấn đề tìm nghiệm hữu tỷ của phương trình $X^2 + Y^2 = 1$.

Theo kết quả câu a) phương trình $X^2 + Y^2 = 1$ cho ta nghiệm hữu tỷ là

$$X = \frac{2k}{k^2+1}, \quad Y = \frac{k^2-1}{k^2+1}$$

với k là một số hữu tỷ. Từ đó nếu đặt $X = \frac{x}{z}$, $Y = \frac{y}{z}$

$k = \frac{m}{n}$, $(m, n) = 1$, $m > n > 0$, m chẵn, n lẻ (hoặc ngược lại) thì ta được

$$x = 2mn,\ y = m^2 - n^2,\ z = m^2 + n^2$$

là nghiệm nguyên dương của phương trình $x^2+y^2=z^2$.

5.35. Nếu các số nguyên x, y thỏa mãn phương trình $x^2 + y^2 = 2z^2$ thì đồng thời x, y chẵn hoặc đồng thời x, y lẻ. Bởi vậy $x + y$ và $x - y$ cùng chẵn. Giả sử $x + y = 2u$, $x - y = 2v$, $u, v \in z$.

Khi ấy:

$$4u^2 + 4v^2 = (x + y)^2 + (x - y)^2 = 2(x^2 + y^2)$$

hay là

$$u^2 + v^2 = z^2.$$

Ngược lại nếu có các số nguyên u, v, z thỏa mãn $u^2 + v^2 = z^2$ thì bằng cách đặt $x = u + v$, $y = u - v$ ta được $x^2 + y^2 = 2z^2$. Phương trình $u^2 + v^2 = z^2$ cho ta chẳng hạn

$u = (m^2 - n^2)t$, $v = 2mnt$, $z = (m^2 + n^2)t$, $t \in z$ nên phương trình đã cho có nghiệm

$$\begin{cases} x = (m^2 - n^2 + 2mn)t, \\ y = (m^3 - n^2 - 2mn)t, \\ z = (m^2 + n^2)t,\ t = 0, \pm 1, \ldots \end{cases}$$

5.37. *Chỉ dẫn:* Chỉ cần chứng tỏ phương trình đã cho không có nghiệm nguyên dương. Chú ý rằng nếu α không chia hết cho 3 thì α^2 chia cho 3 dư là 1, bởi vậy, nếu giả sử phương trình đã cho có nghiệm nguyên $x > 0$, $y > 0$, $z > 0$ thì $x = 3x_1$, $y = 3y_1$. Khi ấy ta có $3x_1^2 + 3y_1^2 = z^2$. Từ đẳng thức này lại có $z = 3z_1$ do đó ta có $x_1^2 + y_1^2 = 3z_1^2$ với $o < z_1 < z$. Điều này sẽ dẫn đến mâu

thuẫn vì với lập luận ở trên, từ sự có nghiệm nguyên dương x, y, z của phương trình đã cho ta lại tìm được vô số nghiệm nguyên dương của nó mà $z > z_1 > z_2 > \ldots > 0$.

5.38. Biến đổi phương trình về dạng $\left(\frac{x}{u}\right)^2 + \left(\frac{y}{u}\right)^2 + \left(\frac{z}{u}\right)^2 = 1$. Bằng cách đặt $\frac{x}{u} = p$, $\frac{y}{u} = q$, $\frac{z}{u} = s$ ta được $p^2 + q^2 + s^2 = 1$, suy ra từ đó chẳng hạn $p = 1$, $q = 0$, $s = 0$ đặt $p = x_1 + 1$, $q = y_1$, $s = z_1$ ta được
$x_1^2 + y_1^2 + z_1^2 + 2x_1 = 0$.

Giả sử $\quad \frac{x_1}{z_1} = \frac{m}{n}$, $\frac{y_1}{z_1} = \frac{r}{n}$.

Trả lời:
$$\begin{cases} x = (r^2 + n^2 - m^2)t, \\ y = 2mrt, \\ z = 2mnt, \\ u = (r^2 + n^2 + m^2)t, \text{ t nguyên dương tùy ý,} \end{cases}$$

hoặc:
$$\begin{cases} x = \dfrac{r^2 + n^2 - m^2}{d}, \\ y = \dfrac{2mr}{d}, \\ z = \dfrac{2mn}{d}, \\ u = \dfrac{r^2 + n^2 + m^2}{d}, \end{cases}$$

trong đó d là ước chung của $r^2 + n^2 - m^2$, $2mr$, $2mn$ và $r^2 + n^2 + m^2$.

5.39. *Trả lời*
$$\begin{cases} x = (p^2 + q^2 + r^2 - s^2)k, \\ y = 2qsk, \\ z = 2rsk, \\ u = 2psk, \\ t = (p^2 + q^2 + r^2 + s^2)k, \end{cases}$$

với k là một số nguyên, hoặc

$$\begin{cases} x = \dfrac{p^2 + q^2 + r^2 - s^2}{d}, \\ y = \dfrac{2qs}{d}, \\ z = \dfrac{2rs}{d}, \\ u = \dfrac{2ps}{d}, \\ t = \dfrac{p^2 + q^2 + r^2 + s^2}{d}, \end{cases}$$

trong đó d là ước chung của $p^2 + q^2 + r^2 - s^2$, $2qs$, $2rs$, $2ps$ và $p^2 + q^2 + r^2 + s^2$.

5.40. *Chỉ dẫn:* Gọi các cạnh kề góc 60° là x, y còn cạnh kia là z, chúng ta được phương trình

$$x^2 - xy + y^2 = z^2.$$

Giải như trên (xem bài 5.38) ta được

$x = (m^2 - n^2)t$, $y = m(m - 2n)t$, $z = (m^2 - mn + n^2)t$, hoặc

$$x = \frac{m^2 - n^2}{d}, \ y = \frac{m(m - 2n)}{d}, \ z = \frac{m^2 - mn + n^2}{d}.$$

5.41. Bài toán dẫn đến giải phương trình

$$x^2 + xy + y^2 = z^2$$

Trả lời: $x = (m^2 - n^2)t$, $y = (2n - m)mt$,

$z = (m^2 - mn + n^2)t$,

hoặc

$$x = \frac{m^2 - n^2}{d}, \ y = \frac{(2n - m)m}{d}, \ z = \frac{m^2 - mn + n^2}{d}.$$

5.44. Giả sử định lý 1 là đúng. Nếu như định lý 2 sai thì có số tự nhiên u, v, $t > 0$ sao cho $u^3 + v^3 = t^3$.

Khi ấy bằng cách đặt $x = u^2v$, $y = v^2t$, $z = t^2u$ chúng ta sẽ có x, y, z là các số tự nhiên khác không thỏa mãn

$$\frac{x}{y} + \frac{y}{z} = \frac{u^2v}{v^2t} + \frac{v^2t}{t^2u} = \frac{u^3 + v^3}{uvt} = \frac{t^3}{uvt} = \frac{z}{x}$$

nghĩa là lại suy ra định lý 1 là sai. Điều này mâu thuẫn.

Ngược lại giả sử định lý 1 là sai. Khi ấy có những số nguyên dương x, y, z sao cho

$$\frac{x}{y} + \frac{y}{z} = \frac{z}{x}$$

nên ta có

$$x^2z + y^2x = z^2y.$$

Giả sử $x^2z = a$, $y^2x = b$ khi đó $z^2y = a + b$ và $ab(a + b) = (zyz)^3$. Giả sử $d = (a, b)$ và $a = a_1 d$, $b = b_1 d$ thì $(a_1, b_1) = 1$ và $a + b = d(a_1 + b_1)$. $a_1b_1(a_1 + b_1)d^3 = (xyz)^3$. Từ đây dẫn đến $d^3 | (xyz)^3$ có nghĩa là $d | xyz$ cho nên $xyz = dt$, trong đó t là một số tự nhiên. Bởi vậy $a_1b_1(a_1 + b_1) = t^3$ mà $(a_1b_1, a_1 + b_1) = 1$ (do $(a_1, b_1) = 1$, hãy xem bài tập 1.19. b)), suy ra từ đó rằng $a_1 = u^3$, $b_1 = v^3$, $a_1 + b_1 = t^3$ với u, v, t là những số nguyên dương. Dễ thấy rằng

$$u^3 + v^3 = t^3,$$

nghĩa là phương trình $u^3 + v^3 = t^3$ có nghiệm nguyên dương. Vậy định lý 2 là sai.

∴

6.1. a) $100a + 10b + c \equiv 0 \pmod{21} \Leftrightarrow 400a + 40b + 4c \equiv 0 \pmod{21}$ (vì $(4,21) = 1$) $\Leftrightarrow a - 2b + 4c + 21(19a + 2b) \equiv 0 \pmod{21} \Leftrightarrow a - 2b + 4c \equiv 0 \pmod{21}$.

b) *Chỉ dẫn:* Sử dụng $3^4 = 81 \equiv 1 \pmod{10}$ và $(81, 10) = 1$.

6.2. a) Số dư là 5.

b) $1532 \equiv 2 \pmod 9$ nên $1532^5 - 1 \equiv 2^5 - 1 \equiv 32 - 1 \equiv 4 \pmod 9$. *Đáp số:* 4.

c) $(12371^{56}+34)^{28} \equiv (50^{56}+34)^{28} \pmod{111}$

$\equiv (16+34)^{28} \equiv 70 \pmod{111}$. *Đáp số*. 70.

6.3. a) $102 = 2 \cdot 3 \cdot 17$. Gọi $A = 220^{119^{69}} + 119^{69^{220}} + 69^{220^{119}}$. Từ $220 \equiv 0 \pmod 2$, $69 \equiv 1 \pmod 2$, $119 \equiv 1 \pmod 2$, suy ra $A \equiv 0 \pmod 2$.

Từ $220 \equiv 1 \pmod 3$, $69 \equiv 0 \pmod 3$, $119 \equiv -1 \pmod 3$ suy ra $A \equiv 0 \pmod 3$.

Từ $220 \equiv -1 \pmod{17}$, $69 \equiv 1 \pmod{17}$, $119 \equiv 0 \pmod{17}$ suy ra $A \equiv 0 \pmod{17}$. Vậy $A \equiv 0 \pmod{102}$.

b) Từ $36 \equiv 5 \pmod{31}$ suy ra $6^{2n+1} \equiv 6.5^n \pmod{31}$. Lại vì $6 \equiv -25 \pmod{31}$ ta có $6^{2n+1} \equiv -25.5^n \pmod{31}$, tức là $6^{2n+1}+5^{n+2} \equiv 0 \pmod{31}$.

6.4. *Chỉ dẫn*. Một số tự nhiên α bao giờ cũng biểu diễn được duy nhất dưới dạng

$$\alpha = a_n \cdot 10^n + a_{n-1} 10^{n-1} + \dots + a_1 \cdot 10 + a_0,$$

trong đó

$$1 \leqslant a_n \leqslant 9 ;\ 0 \leqslant a_i \leqslant 9 \ (i = 0, 1, \dots, n-1)$$

a) $\alpha \equiv 0 \pmod 2 \Leftrightarrow a_0 \equiv 0 \pmod 2$ vì $10 \equiv 0 \pmod 2$. Vậy $\alpha \vdots 2$ khi và chỉ khi $a_0 = 0 ; 2 ; 4 ; 6 ; 8$.

Tương tự $\alpha \vdots 5$ khi và chỉ khi $a_0 = 0, 5$.

b) Vì $10 \equiv 1 \pmod 3$ nên $\alpha \equiv 0 \pmod 3$ khi và chỉ khi $a_n + a_{n-1} + \dots + a_1 + a_0 \equiv 0 \pmod 3$.

Tương tự $\alpha \equiv 0 \pmod 9 \Leftrightarrow a_n + a_{n-1} + \dots + a_1 + a_0 \equiv 0 \pmod 9$.

c) Vì $100 \equiv 0 \pmod 4$ cho nên $\alpha \equiv 0 \pmod 4$ khi và chỉ khi $10a_1 + a_0 \equiv 0 \pmod 4$.

Tương tự ta có $\alpha \equiv 0 \pmod 8$ khi và chỉ khi $100a_2 + 10a_1 + a_0 \equiv 0 \pmod 8$.

d) $\alpha \equiv 0 \pmod 6 \Leftrightarrow \alpha \equiv 0 \pmod 2$ và $\alpha \equiv 0 \pmod 3$ tức là ta có

$$\alpha \equiv 0 \pmod 6 \Leftrightarrow \begin{cases} a_0 = 0, 2, 4, 6, 8; \\ a_0 + a_1 + \dots + a_n \equiv 0 \pmod 3). \end{cases}$$

e) Vì $10 \equiv -1 \pmod{11}$ cho nên ta có $\alpha \equiv 0 \pmod{11}$ khi và chỉ khi $a_0 - a_1 + \dots + (-1)^n a_n \equiv 0 \pmod{11}$.

g) Vì $1000 \equiv -1 \pmod 7$ cho nên ta có $\alpha \equiv 0 \pmod 7$ khi và chỉ khi $100a_2 + 10a_1 + a_0 + (-a_3 + a_4 - \dots + (-1)^n a_n) \equiv 0 \pmod 7$.

6.5. Ta có

$$\begin{cases} 1 \equiv 1 - m \pmod m \\ 2 \equiv 2 - m \pmod m \\ \dots\dots\dots\dots \\ m-2 \equiv m-2-m \pmod m \\ m-1 \equiv m-1-m \pmod m \\ m \equiv -m \pmod m \end{cases}$$

cho nên $\sum_{i=1}^{m} i^n \equiv \sum_{i=1}^{m} (-i)^n \pmod m$.

Nhưng vì n là lẻ ta có $2\sum_{i=1}^{m} i^n \equiv 0 \pmod m$, cho nên $\sum_{i=1}^{m} i^n \equiv 0 \pmod m$ bởi vì $(2, m) = 1$.

6.6. *a)* → *b)*. Giả sử p là một số nguyên tố thế thì $(k, p) = 1$, với mọi $k = 1, 2, \dots, p-1$, nghĩa là $(k!, p) = 1$, $k = 1, 2, \dots, p-1$. Nhưng $C_p^k = \frac{p(p-1)\dots(p-k+1)}{k!} \in Z$, mà $(k!, p) = 1$ cho nên $\frac{(p-1)\dots(p-k+1)}{k!} \in Z$, tức là $C_p^k \equiv 0 \pmod p$.

b) → *c)*. Ta có công thức $C_p^k = C_{p-1}^k + C_{p-1}^{k-1}$ (1) (hãy

thử lại !). Với mỗi $k = 1, 2, \ldots, p-1$ ta có $C_p^k = C_{p-1}^k + C_{p-1}^{k-1} \equiv 0 \pmod p$ nên $C_{p-1}^k \equiv (-1)\, C_{p-1}^{k-1} \pmod p$. Lại áp dụng công thức (1) ta có $C_{p-1}^{k-1} \equiv (-1)(C_p^{k-1} - C_{p-1}^{k-2}) \pmod p$ nên $C_{p-1}^k \equiv (-1)^2\, C_{p-1}^{k-2} \pmod p$ bởi vì $C_p^{k-1} \equiv 0 \pmod p$. Cứ tiếp tục như vậy, cuối cùng ta được $C_{p-1}^k \equiv (-1)^k\, C_{p-1}^0 \pmod p$ hay $C_{p-1}^k \equiv (-1)^k \pmod p$, bởi vì $C_{p-1}^0 = 1$. Mặt khác với $k=0$ ta cũng có

$$C_{p-1}^0 = 1 \equiv (-1)^0 \pmod p.$$

Vậy với mọi $k = 0, 1, \ldots, p-1$ ta đều có $C_{p-1}^k \equiv (-1)^k \pmod p$.

c) $\Rightarrow$ *a*). Áp dụng công thức (1) từ giả thiết $C_{p-1}^k \equiv (-1)^k \pmod p$ $k = 0, 1, \ldots, p-1$ ta có với $k = 1, 2, \ldots, p-1$

$C_p^k \equiv (-1)^k + (-1)^{k-1} \pmod p$, tức là $C_p^k \equiv 0 \pmod p$. Giả sử $p > 1$ không là nguyên tố thì có số nguyên tố r sao cho $2 \leqslant r \leqslant p-1$ và $r \mid p$. Khi ấy theo kết quả ở trên $C_p^r \equiv 0 \pmod p$, nghĩa là $\dfrac{p(p-1)\ldots(p-r+1)}{r!} = pt$ với $t \in \mathbb{Z}$ hay $p(p-1)\ldots(p-r+1) = r!\, pt$. Từ đó ta có $(p-1)(p-2)\ldots(p-r+1) \,\vdots\, r$. Điều này không thể xảy ra bởi vì từ $r \mid p$ ta có $(p-x, r) = (x, r) = 1$ với mọi $x = 1, 2, \ldots, r-1$ (do r là nguyên tố).

Vậy p phải là số nguyên tố.

6.7. Ta có $a = b + m^n t$, $t \in Z$ nên $a^m = b^m + mb^{m-1}m^n t + C_m^2 b^{m-2} m^{2n} t^2 + \ldots + m^{mn} t^m$, tức là $a^m = b^m + km^{n+1} \equiv b^m \pmod{m^{n+1}}$.

6.8. a) Qui nạp theo n. Với $n = 1$ ta có $8 \equiv -1 \pmod 9$.
Giả sử $2^{3^n} \equiv -1 \pmod{3^{n+1}}$ với $n \geq 1$. Khi ấy $2^{3^{n+1}} + 1 = (2^{3^n})^3 + 1 = (2^{3^n} + 1)(2^{2.3^n} - 2^{3^n} + 1) \equiv 0 \pmod{3^{n+2}}$ bởi vì $2^{2.3^n} - 2^{3^n} + 1 \equiv 0 \pmod 3$ (do $2 \equiv -1 \pmod 3$).

Lưu ý. Có thể dựa vào kết quả bài tập 6.7. Thật vậy từ $2 \equiv -1 \pmod 3$ có $2^3 \equiv -1 \pmod{3^2}$. Tiếp tục lại có $2^{3^2} \equiv -1 \pmod{3^3}$,..., và $2^{3^n} \equiv -1 \pmod{3^{n+1}}$.

b) Áp dụng câu a) đã có $2^{3^n} + 1 \equiv 0 \pmod{3^{n+1}}$ nên cũng có $2^{3^n} + 1 \equiv 0 \pmod{3^n}$. Từ đó với $a = 3^n$, $n = 1, 2,\ldots$ ta có $a \mid 2^a + 1$.

6.9. a) Qui nạp theo n. Với $n = 1$ đồng dư thức có dạng $(m-1)^m \equiv -1 \pmod{m^2}$ hay là $(m-1)^m + 1 = m[(m-1)^{m-1} - (m-1)^{m-2} + \ldots + 1] \equiv 0 \pmod{m^2}$, từ đó

$$(m-1)^{m-1} - (m-1)^{m-2} + \ldots + 1 \equiv 0 \pmod m,$$

$$(-1)^{m-1} - (-1)^{m-2} + \ldots + 1 \equiv 0 \pmod m,$$

$$\underbrace{1 + 1 + \ldots + 1}_{m \text{ số hạng}} \equiv 0 \pmod m \qquad \text{(do m là số lẻ)}$$

Đồng dư thức này là hằng đúng và do đó đồng dư thức xuất phát là đúng với m là số lẻ > 1.

Giả sử đồng dư thức cần chứng minh đã đúng với $n \geq 1$. Khi ấy $(m-1)^{m^{n+1}} + 1 = ((m-1)^{m^n})^m + 1 = ((m-1)^{m^n} + 1) \times ((m-1)^{(m-1)m^n} - (m-1)^{(m-2)m^n} + \ldots + 1) \equiv 0 \pmod{m^{n+2}}$ bởi vì $(m-1)^{m^n} + 1 \equiv 0 \pmod{m^{n+1}}$ và

$$(m-1)^{(m-1)m^n} - (m-1)^{(m-2)m^n} + \ldots + 1 \equiv 0 \pmod m$$

(do $m - 1 \equiv -1 \pmod m$ và m là số lẻ).

b) Với $m=5$, đồng dư thức $(m-1)^{m^n} \equiv -1 \pmod{m^{n+1}}$ có dạng $4^{5^n}+1 \equiv 0 \pmod{5^{n+1}}$ từ đó cũng có $4^{5^n}+1 \equiv 0 \pmod{5^n}$ hay $2^{2.5n}+1 \equiv 0 \pmod{5^n}$. Bởi vậy với $a=5^n$, $n = 1, 2,...$ ta có $a \mid 2^{2a}+1$.

6.10. a) Gọi H_i là các hệ thặng dư đầy đủ môđun m_i $(i = 1, 2,..., k)$. Xét $A = \{b + \sum_{i=1}^{k} a_i x_i \mid x_i \in H_i,\ i = 1, 2,..., k\}$. Rõ ràng A có m số. Hơn nữa giả sử $x_i, x_i' \in H_i$ $(i = 1, 2,..., k)$ mà $b + \sum_{i=1}^{k} a_i x_i \equiv b + \sum_{i=1}^{k} a_i x'_i \pmod m$ thế thì ta có $\sum_{i=1}^{k} a_i(x_i - x'_i) \equiv 0 \pmod m$, nên $\sum_{i=1}^{k} a_i(x_i - x_i') \equiv 0 \pmod{m_j}$ $j = 1, 2,..., k$. Nhưng với $i \neq j$ có $a_i \vdots m_j$; $i=j$ có $(a_j, m_j) = 1$, cho nên ta được $x_j - x'_j \equiv 0 \pmod{m_j}$, từ đó $x_j = x'_j$ (vì $x_j, x'_j \in H$) tức là $b + \sum_{i=1}^{k} a_i x_i = b + \sum_{i=1}^{k} a_i x'_i$.

b) Gọi L_i $(i = 1, 2, ..., k)$ là các hệ thặng dư thu gọn môđun m_i. Xét

$$L = \{ \sum_{i=1}^{k} a_i x_i \mid x_i \in L_i,\ i = 1, 2, ..., k, \}.$$

Rõ ràng L gồm tất cả $\varphi(m_1)\,\varphi(m_2)...\,\varphi(m_k)$ số, song $(m_i, m_j) = 1$, $i \neq j$ nên $\varphi(m_1)\,\varphi(m_2)...\,\varphi(m_k) = \varphi(m)$ nghĩa là L gồm có $\varphi(m)$ số.

Như câu a) ta cũng sẽ chứng minh được rằng L gồm các phần tử đôi một không đồng dư với nhau theo môđun m.

Với mỗi i ($i = 1, 2, ..., k$) ta có $(a_i, m_i) = 1$, $(x_i, m_i) = 1$ nên $(a_i x_i, m_i) = 1$. Mặt khác với $i \neq j$ có $a_j \vdots m_i$ cho nên $(\sum_{j=1}^{k} a_j x_j, m_i) = (a_i x_i, m_i) = 1$. Vậy ta có

$$(\sum_{j=1}^{k} a_j x_j, m) = 1.$$

6.11. *Chỉ dẫn:* Giả sử $A = \overline{a}$ là một lớp thặng dư theo môđun m. Xét các lớp thặng dư môđun km sau đây:

$A_o = \overline{a}$, $A_1 = \overline{a + m}$, ..., $A_{k-1} = \overline{a + (k-1)m}$.

Hãy chứng minh $A_i \cap A_j = \phi$ ($i \neq j$, $0 \leqslant i, j \leqslant k - 1$) và $\bigcup_{i=0}^{k-1} A_i = A$.

6.12. Giả sử $\alpha \leqslant \beta$. thế thì $\beta = \alpha + k\varphi(m)$ với $k \in N$. Từ $a^{\varphi(m)} \equiv 1 \pmod m$ ta suy ra rằng $a^{\beta} = a^{\alpha + k\varphi(m)} \equiv a^{\alpha} (\text{mod} m)$.

6.13. a) 3;

b) $\varphi(83) = 82 > 40$. Bởi vậy phải xét

$3^4 = 81 \equiv -2 \pmod{83}$, $3^{40} \equiv (-2)^{10} \pmod{83}$,

$(-2)^{10} = 1024 \equiv 28 \pmod{83}$. *Đáp số:* 28.

c) 2;

d) $3.5^{75} \equiv x \equiv 3 \pmod{132}$; $4.7^{100} \equiv y \equiv 4 \pmod{132}$ nên $x + y \equiv 7 \pmod{132}$. *Đáp số:* 7.

e) $425 = 17.25$; $(35, 425) = 5$. Giả sử $35^{150} \equiv 25x \pmod{17.25}$ ta có $49.35^{148} \equiv x \pmod{17}$. Vì $35^{148} \equiv 1 \pmod{17}$ nên $49.35^{148} \equiv -2 \pmod{17}$, từ đó $35^{150} \equiv 375 \pmod{425}$. *Đáp số:* 375.

g) $10^6 \equiv 1 \pmod 7$; $10^n \equiv 4 \pmod 6$, bởi vậy ta có

$$10^{10} + 10^{10^2} + \dots + 10^{10^{10}} \equiv \underbrace{10^4 + 10^4 + \dots + 10^4}_{10 \text{ số hạng}} \equiv 10^5 \equiv$$

$\equiv 5 \pmod 7$

Đáp số: 5.

6.14. a) *) $2^{999} \equiv 4x \pmod{100}$, $2^{997} \equiv x \pmod{25}$. $997 \equiv -3 \pmod{20}$, $2^{997} \equiv 2^{17} \pmod{25}$, $2^7 = 128 \equiv 3 \pmod{25}$, $2^8 \equiv 6 \pmod{25}$, $2^{16} \equiv 36 \equiv 11 \pmod{25}$, $2^{17} \equiv 22 \pmod{25}$. Vậy $x \equiv 22 \pmod{25}$, $4x \equiv 88 \pmod{100}$. *Đáp số*: 88.

*) $\varphi(100) = 40$; $5^{2k+1} \equiv 5 \pmod{40}$, $5^{1977} \equiv 5 \pmod{40}$

$3^{5^{1977}} \equiv 3^5 \equiv 43 \pmod{100}$. *Đáp số*: 43.

*) $14^{14^{14}} = 7^{14^{14}} . 2^{14^{14}}$. Hãy tìm dư trong phép chia $7^{14^{14}}$ và $2^{14^{14}}$ cho 100.

$7^4 = 2401 \equiv 1 \pmod{100}$, $14^{14} = 2^{14}\, 7^{14} \equiv 0 \pmod 4$ vì vậy $7^{14^{14}} \equiv 1 \pmod{100}$.

$2^{20} \equiv 1 \pmod{25}$; $2^{12} \equiv 1 \pmod{15}$ vì vậy $4.2^{12} = 2^{14} \equiv 4 \pmod{20}$; $7^{12} \equiv 1 \pmod{20}$, $49 \equiv 9 \pmod{20}$ nên $49.7^{12} = 7^{14} \equiv 9 \pmod{20}$. Từ đó chúng ta có $14^{14} \equiv 4.9 \pmod{20}$ hay là $14^{14} = 2^{14} . 7^{14} \equiv 16 \pmod{20}$. Vậy $2^{14^{14}} \equiv 2^{16} \pmod{25}$. Nhưng $2^{16} \equiv 11 \pmod{25}$ còn $2^{14^{14}} \equiv 0 \pmod 4$ nên $2^{14^{14}} \equiv 36 \pmod{100}$. Cuối cùng ta có $2^{14^{14}} . 7^{14^{14}} = 14^{14^{14}} \equiv 36.1 \pmod{100}$.

Đáp số: **36.**

b) $9 \equiv 1 \pmod 8$, $9^9 \equiv 9 \pmod{16}$, $9^{9^9} \equiv 9^9 \pmod{40}$ $9^{9^{9^9}} \equiv 9^{9^9} \pmod{100}$.

Chú ý: Có thể tính toán cụ thể $9^{9^9} \equiv 89 \pmod{100}$.

6.15. a) $2^{12} \equiv 1 \pmod{13}$, $2^{60} \equiv 1 \pmod{13}$. $2^5 \equiv 6 \pmod{13}$, $2^{10} \equiv -3 \pmod{13}$ vậy $2^{70} \equiv -3 \pmod{13}$. Lại có $3^3 \equiv 1 \pmod{13}$, $3^{69} \equiv 1 \pmod{13}$, $3^{70} \equiv 3 \pmod{13}$, cho nên $2^{70} + 3^{70} \equiv 0 \pmod{13}$.

b) $2^5 \equiv -1 \pmod{11}$; $10 \equiv -1 \pmod{11}$ nên $10^5 \equiv -1 \pmod{11}$. Từ đó $20^5 \equiv 1 \pmod{11}$.

$20 \equiv -11 \pmod{31}$; $20^2 \equiv 121 \equiv -3 \pmod{31}$, $20^3 \equiv 33 \equiv 2 \pmod{31}$ nên $20^{15} \equiv 2^5 \equiv 1 \pmod{31}$.

$3^4 \equiv 20 \pmod{61}$, $3^{60} \equiv 20^{15} \pmod{61}$. Nhưng $3^{60} \equiv 1 \pmod{61}$ nên $20^{15} \equiv 1 \pmod{61}$. Vậy $20^{15} \equiv 1 \pmod{11.31.61}$.

c) $3^{4n+1} = 3.3^{4n} = 3.81^n \equiv 3 \pmod{10}$ nên ta có

$2^{3^{4n+1}} \equiv 2^3 \pmod{11}$ và vì vậy $2^{3^{4n+1}} + 3 \equiv 0 \pmod{11}$.

d) $2^6 = 64 \equiv 1 \pmod 9$, $2^{6n} \equiv 1 \pmod 9$, $2^{6n+1} \equiv 4 \pmod 9$ cả hai vế đều chia hết cho 2 nên $2^{6n+2} \equiv 2^3 \pmod{18}$.

Từ đó $2^{2^{6n+2}} \equiv 2^4 \equiv 16 \pmod{19}$, cho nên $2^{2^{6n+2}} + 3 \equiv 0 \pmod{19}$.

e) $1 \leqslant \varphi(n) < n$ nên $n! \equiv 0 \pmod{\varphi(n)}$. Bởi vì $(2, n) = 1$ ta có $2^{\varphi(n)} \equiv 1 \pmod n$. Từ đó ta suy ra $2^{n!} \equiv 1 \pmod n$.

6.16. a) $240 = 2^4 . 3 . 5$, $(a, 2) = (a, 3) = (a, 5) = 1$, $a^4 \equiv 1 \pmod 5$, $a^2 \equiv 1 \pmod{24}$, $a^2 \equiv -1 \pmod 2$ (vì a lẻ) nên $a^4 \equiv 1 \pmod{48}$ (vì $a^4 - 1 = (a^2 - 1)(a^2 + 1)$). Vậy ta có $a^4 \equiv 1 \pmod{5.48}$.

b) Gọi $A = a^{8n} + 3a^{4n} - 4 = (a^{4n} - 1)(a^{4n} - 1 + 5) = a^{4n}(a^{4n} + 3) - 4$.

Từ $a^4 \equiv 1 \pmod 5$ ta có $a^{4n} - 1 \equiv 0 \pmod 5$, bởi vậy từ $A = (a^{4n} - 1)(a^{4n} - 1 + 5)$ ta có $A \equiv 0 \pmod{25}$.

Mặt khác, nếu a chẵn thì $a^4 \equiv 0 \pmod 4$ còn nếu a lẻ thì $a^{4n} + 3 \equiv 0 \pmod 4$ nên từ biểu thức $A = a^{4n}(a^{4n} + 3) - 4$ ta có $A \equiv 0 \pmod 4$, và vì vậy $A \equiv 0 \pmod{100}$.

c) Vì p là nguyên tố lẻ nên $2^p + 1 \equiv 0 \pmod 3$, nên ta có $A = 3^p - 2^p - 1 \equiv 0 \pmod 3$. Lại vì $3^p - 1 \equiv 0$

(mod 2) nên $A \equiv 0$ (mod 2). Vì $3^p - 3 \equiv 0$ (mod p), $2^p - 2 \equiv 0$ (mod p) nên $A = (3^p - 3) - (2^p - 2) \equiv 0$ (mod p).

Nếu $p = 6t + 1$ (vì $p > 7$) thì $A = 3^{6t+1} - 2^{6t+1} - 1 = 3(3^{6t} - 1) - 2(2^{6t} - 1) \equiv 0$ (mod 7) vì $2^6 \equiv 1$ (mod 7), $3^6 \equiv 1$ (mod 7). Nếu $p = 6t + 5$ thì $A = 3^5(3^{6t} - 1) - 2^5(2^{6t} - 1) + 3^5 - 2^5 - 1 \equiv 0$ (mod 7). Vậy $A \equiv 0$ (mod 2, 3, 7, p).

6.17. a) Với $n = 1$ ta có $1 \mid 2^1 - 1$. Giả sử $n > 1$, khi ấy từ $n \mid 2^n - 1$ suy ra n là số lẻ. Gọi p là ước nguyên tố nhỏ nhất của n và d là số mũ nhỏ nhất mà $p \mid 2^d - 1$ thì theo định lý Phécma ta có $d \mid p - 1$ nên $d < p$ và vì vậy cũng theo định lý Phécma ta có $d \mid n$ trái với tính chất của d cho nên không thể $n > 1$. *Đáp số*: $n = 1$.

b) $2^p \equiv 2$ (mod p) nên nếu $2^p \equiv -1$ (mod p) thì $3 \equiv 0$ (mod p), từ đó $p = 3$. Mặt khác với $p = 3$ ta có $2^p + 1 = 9 \equiv 0$ (mod 3). *Đáp số*: $p = 3$.

6.18. Ta có $m^{\varphi(n)} \equiv 1$ (mod n) và $n^{\varphi(m)} \equiv 1$ (mod m), suy ra $m^{\varphi(n)} + n^{\varphi(m)} \equiv 1$ (mod m) và $m^{\varphi(n)} + n^{\varphi(m)} \equiv 1$ (mod n). Từ đó cũng vì $(m, n) = 1$ ta có $m^{\varphi(n)} + n^{\varphi(m)} \equiv 1$ (mod mn).

6.19. Từ $a \equiv 0$ (mod p) ta có $a^{m(p-1)} + a^{n(p-1)} \equiv 0$ (mod p). Đảo lại nếu $a \not\equiv 0$ (mod p) thì $a^{p-1} \equiv 1$ (mod p) cho nên $a^{m(p-1)} + a^{n(p-1)} \equiv 2$ (mod p) nên không thể xảy ra $a^{m(p-1)} + a^{n(p-1)} \equiv 0$ (mod p) bởi vì p là số nguyên tố lẻ.

6.20. Ta có $a_i^2 \equiv a_i$ (mod 2) nên $a_i^4 \equiv a_i^2 \equiv a_i$ (mod 2), $a_i^5 \equiv a_i^2 \equiv a_i$ (mod 2). Lại có $a_i^3 \equiv a_i$ (mod 3) nên $a_i^5 \equiv a_i^3 \equiv a_i$ (mod 3). Cuối cùng vì $a_i^5 \equiv a_i$ (mod 5) nên

$a_i^5 \equiv a_i \pmod{30}$, $i = 1, 2, \ldots, n$. Vậy ta có

$$\sum_{i=1}^{n} a_i^5 \equiv \sum_{i=1}^{n} a_i \equiv 0 \pmod{30}.$$

6.21. b) Gọi $S_m = 1^m + 2^m + \ldots + (p-1)^m$.

Nếu $m \equiv 0 \pmod{p-1}$ tức là $m = k(p-1)$ thì áp dụng định lý Phécma đối với các số hạng của tổng $S_m + 1$ ta được

$S_m + 1 = (1^{k(p-1)} - 1) + (2^{k(p-1)} - 1) + \ldots +$

$+ ((p-1)^{k(p-1)} - 1) + p \equiv 0 \pmod{p}$, nghĩa là $S_m \equiv -1 \pmod{p}$.

Nếu $m \not\equiv 0 \pmod{p-1}$ tức là $m = k(p-1) + r$, $0 < r < p-1$ thì ta có

$$S_m = 1^r (1^{k(p-1)} - 1) + 2^r (2^{k(p-1)} - 1) + \ldots$$
$$+ (p-1)^r ((p-1)^{k(p-1)} - 1) + S_r.$$

Để chứng minh $S_m \equiv 0 \pmod{p}$ ta chỉ cần chứng minh

$$S_r \equiv 0 \pmod{p}.$$

Với $r = 1$ thì $S_1 = \frac{1}{2} p(p-1) \equiv 0 \pmod{p}$ vì p là lẻ.

Giả sử đã có $S_1, S_2, \ldots, S_{r-1} \equiv 0 \pmod{p}$. Khi ấy khai triển tổng $(1+1)^{r+1} + (2+1)^{r+1} + \ldots + (p-1+1)^{r+1}$ ta được $p^{r+1} = p + C_{r+1}^1 S_r + C_{r+1}^2 S_{r-1} + \ldots + C_{r+1}^{r-1} S_1$.

Từ đó suy ra rằng $C_{r+1}^1 S_r \equiv 0 \pmod{p}$. Nhưng $C_{r+1}^1 = r + 1 < p$ nên $(C_{r+1}^1, p) = 1$, vì vậy ta được $S_r \equiv 0 \pmod{p}$.

6.22. a) Nếu $a \neq 1$ thì

$$a^{p-1} + a^{p-2} + \ldots + a + 1 = \frac{a^p - 1}{a-1} = \frac{((a-1)+1)^p - 1}{a-1} =$$

$$= (a-1)^{p-1} + C_p^1 (a-1)^{p-2} + \ldots + C_p^{p-1} \qquad (1)$$

cho nên

— nếu $a - 1 \equiv 0 \pmod{p}$ thì do $C_p^{p-1} \not\equiv 0 \pmod{p^2}$ ta có $a^{p-1} + a^{p-2} + ... + a + 1 \not\equiv 0 \pmod{p^2}$,

— nếu $a - 1 \not\equiv 0 \pmod{p}$ thì $(a - 1)^{p-1} \equiv 1 \pmod{p}$ và lại theo (1) ta có

$$a^{p-1} + a^{p-2} + ... + a + 1 \equiv (a - 1)^{p-1} \pmod{p}$$

nên

$$a^{p-1} + a^{p-2} + ... + a + 1 \not\equiv 0 \pmod{p^2}.$$

Nếu $a = 1$ thì $a^{p-1} + a^{p-2} + ... + a + 1 = p \not\equiv 0 \pmod{p^2}$

b) Nếu $a \equiv 1 \pmod{p^r}$ thì $a^p \equiv 1 \pmod{p^{r+1}}$ (theo bài tập 6.7).

Đảo lại nếu $a^p \equiv 1 \pmod{p^{r+1}}$ thì ta có

$$(a - 1)(a^{p-1} + a^{p-2} + ... + a + 1) \equiv 0 \pmod{p^{r+1}}$$

nhưng theo câu a) ta có

$$a^{p-1} + a^{p-2} + ... + a + 1 \not\equiv 0 \pmod{p^2}$$

nên $a - 1 \equiv 0 \pmod{p^r}$ hay là $a \equiv 1 \pmod{p^r}$.

6.23. a) Gọi $(a, b) = d$, $a = a_1d$, $b = b_1d$, $(a_1, b_1) = 1$.

Giả sử q là ước nguyên tố của $a^n - b^n = d^n (a_1^n - b_1^n)$

— Nếu $q \mid d^n$ thì $q \mid d$ nên $q \mid a - b$, ta có $s = 1$.

— Nếu $q \mid a_1^n - b_1^n$ thì do $(a_1, b_1) = 1$ cũng có $(a_1, q) = (b_1, q) = 1$. Gọi δ là số mũ bé nhất của a_1 và b_1 sao cho $q \mid a_1^\delta - b_1^\delta$, ta sẽ chứng minh $q \mid a_1^m - b_1^m$ thì $\delta \mid m$.

Thật vậy, giả sử $m = \delta t + r$, $0 < r < \delta$. Từ $q \mid a_1^m - b_1^m = a_1^r (a_1^{\delta t} - b_1^{\delta t}) + b_1^{\delta t}(a_1^r - b_1^r)$ suy ra $d \mid a_1^r - b_1^r$, do đó $r = 0$. Với $m = r$ ta được $\delta \mid n$.

— Nếu $0 < \delta < n$ thì $s = \delta$.

— Nếu $\delta = n$ thì theo định lý Phécma ta có

$q \mid (a_1^{q-1} - 1) - (b_1^{q-1} - 1) = a_1^{q-1} - b_1^{q-1}$ suy ra $\delta = n$ là ước của $q - 1$, nghĩa là $q = nk + 1$.

b) Vì $(a, n) = 1$ và $q \mid p$ nên hoặc $\delta = 1$ hoặc $\delta = p$. Ngoài ra $q = pk + 1$ là số nguyên tố lẻ nên k phải là số chẵn, do đó $q = 2kp + 1$.

6.24. a) Gọi $(a, b) = d$, $a = a_1 d$, $b = b_1 d$, $(a_1, b_1) = 1$ ta có $a^n + b^n = d^n (a_1^n + b_1^n)$. Giả sử q là ước nguyên tố của $a^n + b^n$.

– Nếu $q = 2$ hoặc $q \mid d$ thì $q \mid a + b$ (ta có $s = 1$).

– Nếu $q \mid a_1^n + b_1^n$ thì do $(a_1, b_1) = 1$ ta có $(a_1, q) = (b_1, q) = 1$. Gọi δ là số mũ nhỏ nhất sao cho $q \mid a_1^\delta + b_1^\delta$. Trước hết ta chứng minh rằng nếu h là số mũ nhỏ nhất sao cho $q > 2$ mà $q \mid a_1^h - b_1^h$ thì $h = 2\delta$ và như vậy suy ra điều cần chứng minh. Từ $q \mid a_1^\delta + b_1^\delta$ ta có $q \mid a_1^{2\delta} - b_1^{2\delta} = (a_1^\delta + b_1^\delta)(a_1^\delta - b_1^\delta)$. Áp dụng bài tập 6.23 ta có $h \mid 2\delta$. Không thể $h \mid \delta$ vì nếu như vậy thì từ $q \mid a_1^\delta - b_1^\delta = a_1^\delta + b_1^\delta - 2b_1^\delta$ suy ra $q \mid 2b_1^\delta$ và do đó $q \mid 2b_1$ là không được bởi vì $q > 2$ và $(q, b_1) = 1$. Vậy $h = 2^s$ với $s \mid \delta$. Vì $s < h$ và δ là số mũ nhỏ nhất sao cho $q \mid a_1^\delta + b_1^\delta$ nên từ $a_1^{2s} - b_1^{2s} = (a_1^s + b_1^s)(a_1^s - b_1^s)$ suy ra $s = \delta$ tức là $h = 2\delta$.

b) Áp dụng a).

6.25. a) Từ $(a, b) = 1$ và $p \mid a^2+b^2$ ta suy ra $(a, p) = (b, p) = 1$. Giả sử $a^2 + b^2 = pt$ với $p = 2m + 1$ thì $p \mid a^{p-1} - 1 = a^{2m} - 1 = (pt - b^2)^m - 1 = pu + (-b^2)^m - 1 = pu - (-1)^m (b^{p-1} - 1) + (-1)^m - 1$. Từ $p \mid pu - (-1)^m \times (b^{p-1} - 1) + (-1)^m - 1$ và $p \mid b^{p-1} - 1$ ta có $p \mid (-1)^m - 1$ nên phải có m là số chẵn, nghĩa là $m = 2k$ Vậy $p = 4k + 1$.

b) Chứng minh qui nạp theo s, dựa vào câu a).

6.26. a) Giả sử p là một số nguyên tố lẻ cho trước thế thì theo bài tập 6.23 có ước số nguyên tố của $2^p - 1$, ước đó có dạng $2pk + 1$. Giả sử $q_1, q_2, \ldots, q_r$ là các số nguyên tố dạng $2pk+1$. Xét ước nguyên tố lẻ q của số: $\dfrac{a^p - 1}{a - 1}$ trong đó $a = pq_1q_2 \ldots q_r$. Nếu $q \mid a-1$ thì $q \mid \dfrac{a^p - 1}{a - 1} = (a^{p-1} - 1) + (a^{p-2} - 1) + \ldots + (a - 1) + p$ suy ra $q \mid p$ hay $p = q$ là ước của $a - 1 = pq_1q_2 \ldots q_r - 1$. Từ đó p là ước của 1 là không thể được. Vậy không thể q là ước của $a - 1$, vậy q phải có dạng $2kp + 1$ (bài tập 6.23). Rõ ràng $q \neq q_i$, $\forall i = 1, 2, \ldots, r$ vì nếu trái lại thì ta sẽ đi đến $q \mid 1$ là điều không thể được.

b) Tương tự như câu a) bằng cách sử dụng bài tập 6.25.

6.27. *Hướng dẫn*: a) Qui nạp theo a. Trong trường hợp $a = 2$ ta có:

$$(h_1 + h_2)^p = h_1^p + h_2^p + C_p^1 h_1^{p-1} h_2, + \ldots + C_p^{p-1} h_1 h_2^{p-1},$$

trong đó $C_p^k \equiv 0 \pmod p$, $k = 1, 2, \ldots, p - 1$ (xem bài tập 6.6).

b) $$a^p = (\underbrace{1 + 1 + \ldots + 1}_{\text{a số hạng}})^p \equiv \underbrace{1^p + 1^p + \ldots + 1^p}_{\text{a số hạng}} \equiv a \pmod p.$$

c) Giả sử $(a, m) = 1$, $m = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$ thế thì

$$(a, p_i) = 1,\ i = 1, 2, \dots, k,\ a^{p_i - 1} \equiv 1 \pmod{p_i}.$$

Từ đó hãy bằng qui nạp chứng minh

$$(a^{p_i - 1})^{p_i^r} \equiv 1 \pmod{p_i^{r+1}}$$

để đi đến $a^{\varphi(p_i^{\alpha_i})} \equiv 1 \pmod{p_i^{\alpha_i}}$, $i = 1, 2, \dots, k$.

Nhưng $\varphi(m) \equiv 0 \pmod{\varphi(p_i^{\alpha_i})}$ nên ta có

$$a^{\varphi(m)} \equiv 1 \pmod{p_i^{\alpha_i}},\ i = 1, 2, \dots, k.$$

Từ đó

$$a^{\varphi(m)} \equiv 1 \pmod{m}.$$

7.1 a) $x \equiv 37 \pmod{117}$; b) $x \equiv 31 \pmod{183}$; c) Vô nghiệm; d) $x \equiv 1630 \pmod{2413}$;

e) Sau khi thêm vào vế phải số hạng $2ab$ ta được $(a + b)x \equiv (a + b)^2 \pmod{ab}$, $x \equiv a + b \pmod{ab}$ (vì $(a, b) = 1$).

7.2. a) $x \equiv 10, 21, 32 \pmod{33}$,

b) $x \equiv 61, 248 \pmod{422}$,

c) $x \equiv 39, 196, 353 \pmod{471}$,

d) $x \equiv 153, 461, 769 \pmod{924}$

e) Nếu $(a + 1, m) = 1$ thì $x \equiv a - 1 \pmod{m}$.
Nếu $(a + 1, m) = d > 1$ thì ta có

$$x \equiv a - 1,\ a - 1 + \frac{m}{d}, \dots, a - 1 + \frac{(d-1)m}{d} \pmod{m}.$$

7.3. Ta có $p - i \equiv -i \pmod{p}$ nên suy ra rằng
$(p - 1)(p - 2) \dots (p - a + 1) \equiv (-1)^{a-1}(a - 1)! \pmod{p}$.
Từ đó $(a - 1)!\, a \,.\, b\,(-1)^{a-1} \dfrac{(p-1)(p-2 \dots (p-a+1)}{a!} \equiv$
$\equiv b(a - 1)! \pmod{p}$. Song $((a - 1)!, p) = 1$ nên ta được

$$a\left(b(-1)^{a-1}\cdot\frac{(p-1)(p-2)\dots(p-a+1)}{a!}\right)\equiv b \pmod p$$

suy ra điều cần chứng minh.

7.4. Đặt $x_o = \sum_{i=1}^{k} M_i M'_i b_i$ ta có $x_o \equiv b_i \pmod{m_i}$

với mọi $i = 1, 2, \dots, k$ vì $M_j \equiv 0 \pmod{m_i}$ với mọi $j \neq i$

Áp dụng: b) $x \equiv 15a + 21b - 35c \pmod{105}$.

7.5. a) $x \equiv 49 \pmod{420}$; c) vô nghiệm; d) $x \equiv 17 \pmod{90}$.

7.6. a) $x \equiv 4a - 3 \pmod{24}$ với $a \equiv 1 \pmod 2$.

b) Hệ có nghiệm khi và chỉ khi $a \equiv 8 \pmod 7$ hay là $a \equiv 1 \pmod 7$, trong đó $7 = (21, 35)$. Khi ấy

$$x \equiv 216\,a - 355 \pmod{630}$$

7.7 a) Hệ có nghiệm khi và chỉ khi $11 - a \equiv 0 \pmod 2$ và $1 - a \equiv 0 \pmod 3$, trong đó $2 = (18, 20)$, $3 = (18, 15)$. Từ đó $a \equiv 1 \pmod 6$

b) Từ $3x \equiv 4 \pmod{10}$ ta có $x \equiv 8 \pmod{10}$. Phương trình $2x \equiv \pmod 8$ có nghiệm khi và chỉ khi $a \equiv 0 \pmod 2$ tức là $a = 2k$, $k \in Z$. Khi ấy hệ tương đương với hệ

$$\begin{cases} x \equiv 8 \pmod{10}, \\ x \equiv k \pmod 4). \end{cases}$$

Hệ này có nghiệm khi và chỉ khi $k - 8 \equiv 0 \pmod 2$ tức là $k \equiv 0 \pmod 2$ trong đó $2 = (10, 4)$. Thành thử hệ đã cho có nghiệm khi và chỉ khi $a \equiv 0 \pmod 4$.

7.8. Ta phải tìm số nguyên x sao cho $0 \leqslant x < 100$ thỏa mãn hệ

$$\begin{cases} x \equiv 4 \pmod 9), \\ x \equiv 3 \pmod 5), \\ x \equiv 1 \pmod 3), \\ x \equiv 9 \pmod{11}). \end{cases}$$

Hệ này cho ta $x \equiv -167 \pmod{495}$.

Trả lời: $x = 328;\ 823$.

7.9. Bài toán đưa về giải hệ

$$\begin{cases} x \equiv 3 \pmod 7, \\ x^2 \equiv 44 \pmod{7^2}, \\ x^3 \equiv 111 \pmod{7^3}. \end{cases}$$

Thay $x = 3 + 7q$ (xem phương trình đầu) vào phương trình thứ hai ta được $q = 2 + 7q_1$, từ đó ta có $x = 17 + 7^2 q_1$ thỏa mãn hai phương trình đầu. Thay giá trị đó của ẩn vào phương trình thứ ba ta được $q_1 = 7q_2$, từ đây suy ra $x = 17 + 7^3 q_2$ $(q_2 = 0, 1, 2, \ldots)$.

7.10. a) Bài toán đưa đến hệ

$$\begin{cases} x \equiv 1 \pmod m ; \\ x^2 \equiv m + 1 \pmod{m^2}. \end{cases}$$

Thay $x = 1 + mq$ (từ phương trình đầu) vào phương trình thứ hai được $2q \equiv 1 \pmod m$, từ đó $q = 2^{\varphi(m)-1} + mq_1$ và $x = 1 + m \cdot 2^{\varphi(m)-1} + m^2 q$ hay $x \equiv 1 + m \cdot 2^{\varphi(m)-1} \pmod{m^2}$.

b) Bài toán đưa về hệ

$$\begin{cases} x \equiv m - 1 \pmod m, \\ x^2 \equiv 1 \pmod{m^2}, \end{cases}$$

trong đó $m > 1$ và $(m, 2) = 1$.

7.11. *Chỉ dẫn:* $(a_0, m) = 1$ nên ắt có số nguyên a sao cho $aa_0 \equiv 1 \pmod m$. Khi ấy sau khi nhân phương trình xuất phát với a ta được điều mong muốn.

Áp dụng: Đưa phương trình về phương trình

$$4x^3 - 8x - 40 \equiv 0 \pmod{27},$$
$$x^3 - 2x - 10 \equiv 0 \pmod{27}.$$

7.12. Đặt $x = y + a$, khi ấy phương trình đã cho là $(y + a)^n + a_1(y + a)^{n-1} + \ldots + a_n \equiv 0 \pmod m$. Dựa vào khai triển $(y + a)^k$, $k = 1, 2, \ldots, n$ ta được:

$$y^n + (na + a_1) y^{n-1} + \ldots + b_n \equiv 0 \pmod m.$$

Muốn cho phương trình mới không có số hạng bậc $n-1$ thì cần và đủ là $na + a_1 \equiv 0 \pmod{m}$. Nhưng vì $(m, n) = 1$ nên bao giờ cũng có số nguyên a thỏa mãn $na + a_1 \equiv 0 \pmod{m}$.

Áp dụng. $a \equiv 7 \pmod{13}$

$$y^2 + 2y - 2 = 0 \pmod{13}.$$

7.13. *Chỉ dẫn.* Dựa vào định lý Phécma: với mọi số nguyên x_0 ta có $x_0^p \equiv x_0 \pmod{p}$.

Trả lời: $9x^2 + x + 6 \equiv 0 \pmod{11}$.

7.14. a) $x \equiv \pm 6 \pmod{19}$; b) $x \equiv 2;\ 3 \pmod{13}$;

c) $x \equiv \pm 1 \pmod{17}$;

d) Đưa về $(x^2 - 1)(x^2 - 2) \equiv 0 \pmod{13}$.

Đáp số: $x \equiv \pm 1 \pmod{13}$.

7.15. a) $x \equiv -1 \pmod{25}$; b) $x \equiv 10 \pmod{49}$;

c) Đặt $f(x) = 2x^2 - x - 1$. Trước hết ta thấy phương trình $f(x) \equiv 0 \pmod{3}$ có nghiệm duy nhất $x \equiv 1 \pmod{3}$. Xét các lớp $x \equiv 1;\ 4;\ 7 \pmod{9}$ ta thấy $x \equiv 1;\ 4 \pmod{9}$ nghiệm của phương trình $f(x) \equiv 0 \pmod{9}$. Bây giờ lại xét trong các lớp $x \equiv 1,\ 4 \pmod{9}$ xem lớp nào có những nghiệm của phương trình $f(x) \equiv 0 \pmod{27}$. Ta thấy trong các lớp ấy $x \equiv 1;\ 10;\ 19;\ 4;\ 13;\ 22 \pmod{27}$ có $x \equiv 1;\ 4;\ 10; \pmod{27}$ là nghiệm của $f(x) \equiv 0 \pmod{27}$.

Đáp số: $x \equiv 1;\ 4;\ 10 \pmod{27}$.

d) $x \equiv 16 \pmod{27}$.

7.16. a) Vô nghiệm vì phương trình

$$3x^3 + 4x^2 - 7x - 6 \equiv 0 \pmod{5}$$

vô nghiệm.

b) Đáp số $x \equiv \pm 2,\ \pm 12 \pmod{35}$.

7.17. a) $\begin{cases} x = 6 + 19t, \\ y = -12t - 19t^2 - 2,\ t \in \mathbf{Z}; \end{cases}$

$\begin{cases} x = -6 + 19t, \\ y = 12t - 19t^2 - 2, \quad t \in \mathbf{Z}. \end{cases}$

b) $\begin{cases} x = -1 + 25t, \\ y = 3t - 75t^2 + 625t^3, \ t \in \mathbf{Z}. \end{cases}$

7.18. Giả sử $x^p - x = f(x)\,q(x) + r(x)$, trong đó hoặc $r(x) = 0$ hoặc bậc $r(x) < n$, $q(x)$ có hệ số nguyên.

Giả sử $f(x)$ có đủ n nghiệm $\alpha_1, \alpha_2, \ldots, \alpha_n$ (mod p) khi ấy nếu $r(x) \neq 0$ thì bậc $r(x) < n$ và $r(x) \equiv 0$ (mod p) có ít nhất n nghiệm đó là $\alpha_1, \alpha_2, \ldots, \alpha_n$ (mod p). Từ đó mọi hệ số của $r(x)$ đều là bội của p.

Đảo lại giả sử mọi hệ số của $r(x)$ đều là bội của p thế thì từ $x^p - x = f(x)\,q(x) + r(x) \equiv 0$ (mod p), $\forall x \in \mathbf{Z}$, ta có $f(x)\,q(x) \equiv 0$ (mod p), $\forall x$ (*). Bởi vậy nếu gọi n_1 là số nghiệm của $f(x) \equiv 0$ (mod p), n_2 là số nghiệm của $q(x) \equiv 0$ (mod p) ta có $n_1 \leqslant n$, $n_2 \leqslant p - n$, từ đó $n_1 + n_2 \leqslant p$. Mặt khác từ (*) ta có $n_1 + n_2 \geqslant p$, cho nên $n_1 + n_2 = p$, hay $n_1 = p - n_2 \geqslant n$. Vậy $n = n_1$.

7.19. Giả sử $x^n \equiv a$ (mod p) có nghiệm, khi ấy có số nguyên x_0 sao cho $x_0^n \equiv a$ (mod p). Khi ấy $(x_0, p) = 1$ (vì đã có $(a, p) = 1$) nên $x_0^{p-1} \equiv 1$ (mod p), bởi vậy

$$a^{\frac{p-1}{n}} \equiv 1 \ (\text{mod } p).$$

Ngược lại nếu $a^{\frac{p-1}{n}} \equiv 1$ (mod p) thì khi ấy do $p - 1 = nt$, $t \in \mathbf{N}$ ta có

$$x^p - x = x\,(x^{nt} - a^t) + \left(a^{\frac{p-1}{n}} - 1\right) x$$ tức là dư

$r(x) = \left(a^{\frac{p-1}{n}} - 1\right) x$ trong phép chia $x^p - x$ cho $x^n - a$

có hệ số là bội của p. Áp dụng kết quả bài tập 7.18 phương trình $x^n \equiv a \pmod p$ có đủ n nghiệm.

7.20. a) Áp dụng bài tập 7.19.

b) Theo câu a) nếu phương trình $x^2 \equiv a \pmod p$ có nghiệm thì $a^{\frac{p-1}{n}} \equiv 1 \pmod p$. Hãy xét đồng dư thức

$$a^{p-1} - 1 = \left(a^{\frac{p-1}{2}} - 1\right)\left(a^{\frac{p-1}{2}} + 1\right) \equiv 0 \pmod p.$$

Từ giả thiết phương trình $x^2 = a \pmod p$ vô nghiệm ta sẽ chứng minh được rằng $a^{\frac{p-1}{2}} \not\equiv 1 \pmod p$. Từ đó ta suy ra $a^{\frac{p-1}{2}} \equiv -1 \pmod p$.

7.21. Phương trình đã cho tương đương với

$$(2ax + b)^2 \equiv b^2 - 4ac \pmod p. \qquad (*)$$

a) Nếu $b^2 - 4ac \equiv 0 \pmod p$ thì từ (*) ta suy ra $2ax + b \equiv 0 \pmod p$. Nhưng p là số nguyên lẻ và $(a, p) = 1$ ta được $x \equiv -b(2a)^{p-2} \pmod p$ là nghiệm duy nhất của phương trình đã cho.

b) Giả sử $b^2 - 4ac \not\equiv 0 \pmod p$ thì phương trình (*) có nghiệm khi và chỉ khi $(b^2 - 4ac)^{\frac{p-1}{2}} \equiv 1 \pmod p$ (xem bài tập 7.19).

7.22. Áp dụng bài tập 7.19. Phương trình đã cho có nghiệm khi và chỉ khi $(-1)^{\frac{p-1}{2}} \equiv 1 \pmod p$. Vì p là số nguyên tố lẻ nên $-1 \not\equiv 1 \pmod p$ cho nên đồng dư

thức trên xảy ra khi và chỉ khi $(-1)^{\frac{p-1}{2}} = 1$ tức là $\frac{p-1}{2} = 2k$, $p = 4k + 1$.

7.23. Giả sử cho trước r số nguyên tố dạng $4k + 1$ là $p_1, p_2, ..., p_r$. Khi ấy số $a = (2p_1p_2...p_r)^2 + 1 > 1$ nên a có ước nguyên tố p. Rõ ràng $p \neq 2$, và như vậy từ $(2p_1 p_2...p_r)^2 + 1 \equiv 0 \pmod p$ ta có p phải có dạng $4k + 1$ (bài tập 7.22). Hiển nhiên $p \neq p_i$, $\forall_i = 1, 2, ..., r$, vì nếu trái lại sẽ có $p \mid 1$ là điều vô lý.

7.24. a) Giả sử $\{x_1, x_2, ..., x_{p-1}\}$ là một hệ thặng dư thu gọn môđun p, $x_ix'_i \equiv 1 \pmod p$ $i = 1, 2, ..., p-1$. Khi ấy ta có $\{x'_1, x'_2, ..., x'_{p-1}\}$ cũng là một hệ thặng dư thu gọn môđun p. Thật vậy, rõ ràng $(x'_i, p) = 1$, với mọi $i = 1, 2, ..., p-1$. Hơn nữa nếu $x'_i \equiv x'_j \pmod p$ thì $x'_ix_ix_j \equiv x'_jx_ix_j \pmod p$ tức là $x_i \equiv x_j \pmod p$ từ đó $i = j$ nói khác đi $x'_i = x'_j$.

b) Ta có $x_i = x'_i$ khi và chỉ khi $x_i \equiv 1; p-1 \pmod p$

Thật vậy $x_i = x'_i$ khi và chỉ khi $x_i^2 \equiv 1 \pmod p$ $x_i \equiv \pm 1 \pmod p$ tức là $x_i \equiv 1;\ p-1 \pmod p$.

Từ kết quả đó suy ra điều cần phải chứng minh.

c) Giả sử p là một số nguyên tố, ta đã có
$(p-2)! - 1 \equiv 0 \pmod p$.
Từ đó suy ra

$$(p-1)! - (p-1) \equiv 0 \pmod p$$

tức là

$$(p-1)! + 1 \equiv 0 \pmod p.$$

7.25. *Cách thứ nhất.* Ta có $\{1, 2, ..., p-1\}$ và $\left\{\pm 1, \pm 2, ..., \pm \frac{p-1}{2}\right\}$ là hai hệ TDTG mod p nên ta có

$$1.2...(p-1) \equiv (-1)^{\frac{p-1}{2}} . 1^2 . 2^2 ... \left(\frac{p-1}{2}\right)^2 \pmod p$$

$$\left(\left(\frac{p-1}{2}\right)!\right)^2 \equiv (-1)^{\frac{p-1}{2}} (p-1)! \pmod p.$$

Nhưng $(p-1)! \equiv -1 \pmod p$ và $\frac{p-1}{2} \equiv 0 \pmod 2$ cho nên

$$\left(\left(\frac{p-1}{2}\right)!\right)^2 + 1 \equiv 0 \pmod p.$$

Nói khác đi, $x \equiv \pm\left(\frac{p-1}{2}\right)! \pmod p$ là hai nghiệm của phương trình $x^2 + 1 \equiv 0 \pmod p$.

Cách thứ hai. Ta có $-2k \equiv 2k+1 \pmod{4k+1}$

$$-2k+1 \equiv 2k+2 \pmod{4k+1}$$

$$\cdots\cdots\cdots$$

$$-1 \equiv 4k \pmod{4k+1}.$$

Từ đó $(-1)^{2k}(2k)! \equiv (2k+1)(2k+2)...(4k) \pmod{4k+1}$

$$((2k)!)^2 \equiv (4k)! \pmod{4k+1}.$$

Nhưng $p = 4k+1$ nên $(4k)! = (p-1)! \equiv -1 \pmod p$. do đó ta được

$$\left(\left(\frac{p-1}{2}\right)!\right)^2 + 1 \equiv 0 \pmod p.$$

Áp dụng: a) Phương trình $x^2 + 1 \equiv 0 \pmod{13}$ có nghiệm là $x \equiv \pm 6! \pmod{13}$, tức là $x \equiv \pm 5 \pmod{13}$.

Trả lời: $\begin{cases} x = 5 + 13t, \\ y = -2 - 10t - 13t^2, \end{cases} \quad t \in \mathbb{Z};$

$\begin{cases} x = -5 + 13t, \\ y = -2 + 10t - 13t^2, \end{cases} \quad t \in \mathbb{Z}.$

b) $\begin{cases} x = 4 + 17t, \\ y = 1 + 8t + 17t^2, \end{cases} \quad t \in \mathbb{Z};$

$\begin{cases} x = -4 + 17t, \\ y = 1 - 8t + 17t^2. \end{cases} \quad t \in \mathbb{Z}.$

Bảng các số nguyên tố không vượt quá 4000

2	3	5	7	11	13	17	19
23	29	31	37	41	43	47	53
59	61	67	71	73	79	83	89
97	101	103	107	109	113	127	131
137	139	149	151	157	163	167	173
179	181	191	193	197	199	211	223
227	229	233	239	241	251	257	263
269	271	277	281	283	293	307	311
313	317	331	337	347	349	353	359
367	373	379	383	389	397	401	409
419	421	431	433	439	443	449	457
461	463	467	479	487	491	499	503
509	521	523	541	547	557	563	569
571	577	587	593	599	601	607	613
617	619	631	641	643	647	653	659
661	673	677	683	691	701	709	719
727	733	739	743	751	757	761	769
773	787	797	809	811	821	823	827
829	839	853	857	859	863	877	881
883	887	907	911	919	929	937	941
947	953	967	971	977	983	991	997
1009	1013	1019	1021	1031	1033	1039	1049
1051	1061	1063	1069	1087	1091	1093	1997
1103	1109	1117	1123	1129	1151	1153	1163
1171	1181	1187	1193	1201	1213	1217	1223
1229	1231	1237	1249	1259	1277	1279	1283
1289	1291	1297	1301	1303	1307	1319	1321
1327	1361	1367	1373	1381	1399	1409	1423

1427	1429	1433	1439	1447	1451	1453	1459
1471	1481	1483	1487	1489	1493	1499	1511
1523	1531	1543	1549	1553	1559	1567	1571
1579	1583	1597	1601	1607	1609	1613	1619
1621	1627	1637	1657	1663	1667	1669	1693
1697	1699	1709	1721	1723	1733	1741	1747
1753	1759	1777	1783	1787	1789	1801	1811
1823	1831	1847	1861	1867	1871	1873	1877
1879	1889	1901	1907	1913	1931	1933	1949
1951	1973	1979	1987	1993	1997	1999	2003
2011	2017	2027	2029	2039	2053	2063	2069
2081	2083	2087	2089	2099	2111	2113	2129
2131	2137	2141	2143	2153	2161	2179	2203
2207	2213	2221	2237	2239	2243	2251	2267
2269	2273	2281	2287	2293	2297	2309	2311
2333	2339	2341	2347	2351	2357	2371	2377
2381	2383	2389	2393	2399	2411	2417	2423
2437	2441	2447	2459	2467	2473	2477	2503
2521	2531	2539	2543	2549	2551	2557	2579
2591	2593	2609	2617	2621	2633	2647	2657
2659	2663	2671	2677	2683	2687	2689	2693
2699	2707	2711	2713	2719	2729	2731	2741
2749	2753	2767	2777	2789	2791	2797	2801
2803	2819	2833	2837	2843	2851	2857	2861
2879	2887	2897	2903	2909	2917	2927	2939
2953	2957	2963	2969	2971	2999	3001	3011
3019	3023	3037	3041	3049	3061	3067	3079
3083	3089	3109	3119	3121	3137	3163	3167
3169	3181	3187	3191	3203	3209	3217	3221
3229	3251	3253	3257	3259	3271	3299	3301
3307	3313	3319	3323	3329	3331	3343	3347
3359	3361	3371	3373	3389	3391	3407	3413
3433	3449	3457	3461	3463	3467	3469	3491
3499	3511	3517	3527	3529	3533	3539	3541
3547	3557	3559	3571	3581	3583	3593	3607
3613	3617	3623	3631	3637	3643	3659	3671
3673	3677	3691	3697	3701	3709	3719	3727
3733	3739	3761	3767	3769	3779	3793	3797
3803	3821	3823	3833	3847	3851	3853	3863
3877	3881	3889	3907	3911	3917	3919	3923
3929	3931	3943	3947	3967	3989 ;		

TÀI LIỆU THAM KHẢO

1. *Lại Đức Thịnh:* Số luận. Tập 1. Nhà xuất bản giáo dục Hà nội, 1969.

2. *Lại Đức Thịnh:* Số luận. Tập 2. Nhà xuất bản giáo dục. Hà nội, 1969.

3. *Lại Đức Thịnh:* Giáo trình số học. Nhà xuất bản giáo dục Hà nội, 1977.

4. *Hoàng Xuân Sính:* Đại số cao cấp. Tập 2 – Nhà xuất bản giáo dục – Hà nội, 1977.

5. И. М. ВИНОГРАДОВ. Основы теории чисел. Москва, 1965.

6. В. СЕРПИНСКИЙ. О решении уравнении в целых числах. Москва, 1961.

7. В. СЕРПИНСКИЙ. Что мы знаем и чего не знаем о простых числах. Москва, 1963.

8. В. СЕРПИНСКИЙ. 250 задач по элементарной теории чисел. Москва, 1968.

9. А.К. СУШКЕВИЧ. Теория чисел. Харьков, 1956.

10. А. О. ГЕЛЬФОНД. Рещение уравнение в целых числах. Моска, 1978.

11. Г.ДЭВЕНПОРТ. Высшая арифметика. Москва, 1965.

12. А.Я. ХИНЧИН. Элементы теории чисел. Москва–Ленинград, 1951.

13. А.Я. ХИНЧИН. Цепные дроби. Москва, 1978.

14. Ш.Х. МИХЕЛОВИЧ. Теория чисел. Москва, 1967.

15. ЭРНСТ ТРОСТ. Простые числа. Москва, 1959.

16. Г. А. КУДРЕВАТОВ. Сборник задач по теории чисел. Москва, 1970.

17. В.У. ГРИБАНОВ, П.И. ТИТОВ. Сборник упражнений по теории чисел. Москва, 1964.

18. Д. О. ШКЛЯРСКИЙ, Н. Н. ЧЕНЦОВ, И.М. ЯГЛОМ. Избранные задачи и теоремы элементарной математики. Арифметика и алгебра. Москва, 1976.

19. У.С ДАВЫДОВ. Задачи и упражнения по теоретической арифметике целых чисел. Минск, 1963.

MỤC LỤC

NGUYỄN HỮU HOAN

SỐ HỌC PHỔ THÔNG

Biên tập: NGUYỄN VĂN GIANG

Trình bày: SỸ KHƯƠNG

In 10 000 cuốn, khổ 13 × 19 tại nhà máy in Diên Hồng, Hà Nội
Số XB44/ĐH. Số in 140/T2. In xong và nộp lưu chiểu tháng 12-1986